Strategic Intelligence, Volumes 1–5

Edited by
Loch K. Johnson

PRAEGER SECURITY INTERNATIONAL

STRATEGIC INTELLIGENCE

STRATEGIC INTELLIGENCE

1

UNDERSTANDING THE HIDDEN SIDE OF GOVERNMENT

Edited by
Loch K. Johnson

Intelligence and the Quest for Security

PRAEGER SECURITY INTERNATIONAL
Westport, Connecticut • London

Library of Congress Cataloging-in-Publication Data

Strategic intelligence / edited by Loch K. Johnson.
p. cm.—(Intelligence and the quest for security, ISSN 1932-3492)
Includes bibliographical references and index.
ISBN 0-275-98942-9 (set : alk. paper)—ISBN 0-275-98943-7 (vol. 1 : alk. paper)—
ISBN 0-275-98944-5 (vol. 2 : alk. paper)—ISBN 0-275-98945-3 (vol. 3 : alk. paper)—
ISBN 0-275-98946-1 (vol. 4 : alk. paper)—ISBN 0-275-98947-X (vol. 5 : alk. paper)
1. Military intelligence. 2. Intelligence service—Government policy. I. Johnson, Loch K., 1942–

UB250.S6385 2007
327.12—dc22 2006031165

British Library Cataloguing in Publication Data is available.

Library of Congress Catalog Card Number: 2006031165
ISBN: 0-275-98942-9 (set)
0-275-98943-7 (vol. 1)
0-275-98944-5 (vol. 2)
0-275-98945-3 (vol. 3)
0-275-98946-1 (vol. 4)
0-275-98947-X (vol. 5)
ISSN: 1932-3492

First published in 2007

Praeger Security International, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the Untied States of America

The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE

THIS FIVE-VOLUME SERIES IN INTELLIGENCE IS SOMETHING of a landmark in the study of intelligence. Thirty years ago, one would have been hard-pressed to find enough good articles on the subject to fill two volumes, let alone five. In those three decades since 1975, however, the study of intelligence has grown considerably. Today there are several solid professional journals in the field, including the premier publications *Intelligence and National Security* (published in the United Kingdom), *International Journal of Intelligence and Counterintelligence* (the United States), and *Studies in Intelligence* (from the Central Intelligence Agency, in both classified and unclassified form). In just the past two years, bulging anthologies on the general topic "strategic intelligence," as well as a "handbook" on intelligence and a collection of chapters within the more specialized niche of "intelligence and ethics" have appeared, along with a tidal wave of books and articles on one aspect or another of this subject (see the bibliographic essay in volume 1).

Except in times of scandal (Watergate in 1973, CIA domestic spying in 1974, the Iran-*contra* affair in 1987), one could find in this earlier era little newspaper coverage of intelligence activities, so tightly held were these operations by the government. Now, fueled by the events of the September 11, 2001, terrorist attacks and the erroneous prediction in 2002 that weapons of mass destruction (WMDs) were being developed and stockpiled by Iraq, hardly a week goes by without reports on intelligence in the *New York Times* and other leading newspapers. These days, the *Atlantic Monthly* and the *New Yorker*, America's top literary magazines, visit the subject with some regularity, too. The latter has hired Seymour M. Hersh, the nation's most well-known investigative reporter with an intelligence beat.

Intelligence studies has come of age.

Certainly the chapters in these volumes display a breadth of inquiry that suggests an admirable vibrancy in this relatively new field of study. Presented here are empirical inquiries, historical treatments, theoretical frameworks, memoirs, case studies, interviews, legal analyses, comparative essays, and ethical assessments. The authors come from the ranks of academe (twenty-five); the intelligence agencies (thirteen); think tanks (seven); Congress, the State Department, and the National Security Council (three); and the legal world (three).[1] Over a quarter of the contributors are from other nations, including Canada, England, Germany, Israel, Scotland, Switzerland, and Wales. The American writers come from every region of the United States. As a collective, the authors represent a wide range of scholarly disciplines, including computer science, history, international affairs, law, sociology, political science, public administration, public policy studies, and strategic studies. Many of the contributors are from the ranks of the top intelligence scholars in the world; a few young ones stand at the gateway to their academic careers.

Notable, too, is the number of women who have entered this field of study. Thirty years ago, it would have been rare to find one or two women writing on this subject. Seven have contributed chapters to these pages, and another two wrote documents that appear in the appendixes. This is still fewer than one would like, especially in light of the major contribution women have made as intelligence officers. One thinks of the heroic efforts of British women in code breaking and in the Special Operations Executive during World War II, and the American women who contributed so much to the analytic efforts of the Office of Strategic Studies (OSS) during that same war. At least, though, the number attracted to the scholar study of intelligence appears to be rapidly expanding.

The end result of this mix is a landscape illuminated by a variety of methods and appreciations—a rich research trove that examines all the key aspects of intelligence. In addition, each of the volumes contains backup materials in the appendixes. These documents provide the reader with access to significant primary and secondary sources referred to in the chapters.

The volumes are organized according to the major topics of studies in the field. The first volume, titled *Understanding the Hidden Side of Government*, introduces the reader to methods commonly used in the study of intelligence. It imparts, as well, a sense of the "state of the discipline," beginning with a bibliographic essay (by the editor) and continuing with an examination of specific approaches scholars have adopted in their inquiries into this especially difficult discipline, where doors are often shut against outsiders.

In the bibliographic essay that opens the volume, I argue that the literature on intelligence has mushroomed over the past thirty years. Some of this literature is unreliable, but much of it is of high quality. Amy B. Zegart follows my chapter with an important caveat: the literature may be more voluminous these days, but intelligence studies as an academic field has yet to be accepted as a vital part of national security scholarship. The mainstream journals of history, international

affairs, and political science have still regarded the study of intelligence as a marginal pursuit. In this regard, Zegart points out, there is a major disconnect between academic scholarship and those who make decisions in Washington, London, and other capitals around the world.

Following this introduction, Len Scott and Timothy Gibbs look at methods that have been used to study intelligence in the United Kingdom; Stuart Farson and Reg Whitaker in Canada; and Michael Warner in the United States. The volume then turns to a more specific inquiry into the central question of how intelligence is interpreted by professionals—the issue of analysis—explored by John Hollister Hedley. An overview of the sometimes turbulent relationship between intelligence officers and the policy makers they serve is explored by James J. Wirtz; and British scholar Peter Gill recalls the failures associated with the 9/11 attacks and the poor judgments about Iraqi WMDs, in hopes of extracting lessons from these intelligence disasters. In the next chapter, the youngest scholar represented in this collection, Harold M. Greenberg, takes us back in time with a remembrance of the legendary CIA officer and Yale history professor Sherman Kent, often known as the dean of CIA analysts. Kristin Lord rounds out the first volume with a look forward into future prospects for a more transparent world—the ultimate goal of intelligence.

As with each of the books, Volume 1 has a set of appendixes designed to supplement the original chapters with supportive materials from government documents and other sources. Appendix A contains the relevant intelligence excerpts from the National Security Act of 1947—the founding charter for the modern American intelligence establishment. Appendix B provides a history of U.S. intelligence since 1947, prepared for the Aspin-Brown Commission in 1995–96 by staff member Phyllis Provost McNeil. These two documents present a contextual backdrop for the Volume 1 chapters. Appendix C provides "wiring diagrams" of the intelligence community, that is, organizational blueprints for the sixteen agencies and related entities. One chart displays the community as it is today, and another displays how it looked in 1985. As the contrast between the two illustrates, the events of September 11, 2001, have led to a larger and more complex intelligence apparatus in the United States. Appendix D shows a photograph of the CIA Headquarters Building, as an example of what one of the secret agencies actually looks like from an aerial perspective. The white dome in the foreground is an assembly hall seating around 600 people and to its left is the main entrance to the original CIA headquarters, built during the Eisenhower years. Behind this older wing is the new green-glass structure erected during the Reagan administration, often known as the Casey addition because William J. Casey was the Director of Central Intelligence (DCI) at the time of its construction during the 1980s.

Appendix E lists the top leadership in the America's intelligence community: the DCIs from 1947–2005 and today's DNI. Included here as well are the leaders in Congress who have been responsible for intelligence accountability in the past, along with the current members of the two congressional Intelligence

Committees: the Senate Select Committee on Intelligence (SSCI, or "sissy" in the unflattering and sometimes true homophone of Capitol Hill vernacular) and the House Permanent Select Committee on Intelligence (HPSCI or "hipsee"). Appendix F presents a 1955 statement from historian and CIA analyst Sherman Kent about the need for a more robust intelligence literature. He would probably be amazed by how much is being written on this subject now. Appendix G offers an overview on the purpose and challenges of intelligence, drawn from the introductory chapters of the Aspin-Brown Commission Report. Finally, Appendix H provides an opening glimpse into the subject of counterintelligence, a world of counterspies and betrayal taken up more fully in Volume 4.

With the second volume, titled *The Intelligence Cycle: The Flow of Secret Information From Overseas to the Highest Councils of Government*, the focus shifts from a broad overview of intelligence to a more detailed examination of its core mission: the collection, analysis, and dissemination of information from around the world. The National Security Act of 1947, which created America's modern intelligence establishment, made it clear that the collection, analysis, and dissemination of information would be the primary duty of the intelligence agencies. As Allen Dulles—the most famous DCI (America's top intelligence official, until this title changed to director of National Intelligence or DNI in 2005)—put it, the intelligence agencies were expected "to weigh facts, and to draw conclusions from those facts, without having either the facts or the conclusions warped by the inevitable and even proper prejudices of the men whose duty it is to determine policy."[2] The collection and interpretation of information, through espionage and from the public record, would be the primary responsibility of America's secret agencies.

At the heart of this mission lies the so-called intelligence cycle. Professional intelligence officers define the cycle as "the process by which information is acquired, converted into intelligence, and made available to policymakers."[3] The cycle has five phases: planning and direction, collection, processing, production and analysis, and dissemination (see Appendix A in Volume 2 for a depiction). As former CIA officer Arthur S. Hulnick notes, however, in the opening chapter, the idea of a "cycle" fails to capture the complexity of how intelligence is collected, assessed, and distributed by intelligence officers.

The next five chapters in Volume 2 take us into the world of the "ints," that is, the specialized "intelligences" (methods) used by intelligence officers to collect information. Patrick Radden Keefe and Matthew M. Aid probe the method of signals intelligence or SIGINT, a generic term used to describe the interception and analysis of communications intelligence and other electronic emissions, from wiretapping telephones to studying the particles emitted by missiles in test flights. Both authors are sensitive to the possible abuse of these techniques, which can be and have been used to spy on Americans without a proper judicial warrant. Jeffrey T. Richelson explores the IMINT domain, that is, imagery intelligence or, in simple terms, photographs taken by surveillance satellites and reconnaissance airplanes (piloted and unpiloted). Telephone conversations can be revealing, but

in the old saying, a picture can be worth a thousand words. (Appendix B provides photographic examples of these spy platforms, and Appendix C offers illustrations of the IMINT data they can collect.)

Important, too, is information that can be acquired by human agents ("assets") guided by case officers inside the CIA or the Defense Department, the topic of human intelligence or HUMINT, examined by Frederick P. Hitz. Not all the information needed by policy makers is acquired through SIGINT, IMINT, or HUMINT; indeed, the overwhelming majority—upward of 95 percent—is already in the public domain. This open-source intelligence (OSINT) must be sorted through, organized, and integrated with the secretly gained information. Robert David Steele's chapter looks at OSINT and its ties to the other ints.

In the next chapter, Daniel S. Gressang IV dissects some of the technological challenges faced by intelligence agencies in sorting through the avalanche of data that pours into their headquarters from various intelligence collectors around the world. Here is the Herculean task of sorting out the wheat from the chaff (or the signal from the noise, in another widely used metaphor) in the search for information that may warn the nation of impending peril. Here is the vital task of providing "indicators and warnings" (I&W) to a nation's leaders.

One of the most difficult relationships in the complex process of collection, analysis, and dissemination of information comes at the intersection between intelligence professionals and policy makers—groups of individuals that often have very different training, aspirations, and cultures. Jack Davis sheds light on this often turbulent relationship in the United States, and Michael Herman tackles the same topic in the United Kingdom. Minh A. Luong offers a case study on economic intelligence that underscores some of the difficulties encountered as information travels from the collectors and analysts (the "producers" of intelligence) to the policy makers (the "consumers"). Finally, Max M. Holland takes a look at how intelligence agencies examine their own mistakes ("postmortems") and attempt to make corrections—and how political consideration enter into the process.

By way of supporting documentation, in addition to the appendixes already mentioned, Appendix D outlines the general types of reports prepared by the producers of intelligence, along with a listing of specific examples. Appendixes E and F provide samples of key intelligence products: National Intelligence Estimates (NIEs)—the most important long-range and in-depth forecasting carried out by the U.S. secret agencies ("research intelligence," in contrast to shorter intelligence reports that tend to focus on near-term events, or "current intelligence"); Special National Intelligence Estimates (SNIEs), which concentrate on a narrow, high-priority information requirement (say, the capabilities of the Chinese military); and the *President's Daily Brief* (PDB), the most exclusive current intelligence report prepared by the intelligence agencies for the consumption of the president and a few other high-ranking officials.

In light of the fact that every study of the 9/11 and Iraqi WMD intelligence failures find fault, in part, with America's capacity for human intelligence—

especially in the Middle East and Southwest Asia—Appendix G presents one of the most searing critiques of this int. The critique, by the House Permanent Select Committee on Intelligence, has become all the more significant because the panel's chairman, Representative Porter Goss (R-FL), soon after the completion of the report rose to the position of the DCI. Last, Appendix H provides an excerpt from a key report on the Iraqi WMD mistakes, prepared by the "Roberts Committee": the Senate Select Committee on Intelligence, led by Pat Roberts (R-KS).

The third volume, titled *Covert Action: Behind the Veils of Secret Foreign Policy*, enters an especially controversial compartment of intelligence: the means by which the United States attempts to not just gather and analyze information about the world—hard enough—but to manipulate global events through secret activities in the advancement of America's best interests. An ambiguous passage of the National Security Act of 1947 charged the National Security Council (NSC), the boss over the sixteen U.S. secret agencies, to "perform such other functions and duties related to intelligence [over and beyond collection-and-analysis] affecting the national security as the National Security Council may from time to time direct."[4] The phrase "other functions and duties" left the door open for launching the CIA (and more recently the Pentagon) on a wide range of covert actions around the world.

Covert action (CA), sometimes referred to as the "quiet option," is based on the supposition that this secret approach to foreign affairs is likely to be less noisy and obtrusive than sending in the Marines. Sometimes professional practitioners also refer to covert action as the "third option," between diplomacy and open warfare. As former Secretary of State and National Security Adviser Henry Kissinger once put it: "We need an intelligence community that, in certain complicated situations, can defend the American national interest in the gray areas where military operations are not suitable and diplomacy cannot operation."[5] Still others prefer the euphemism "special activities" to describe covert action. Whatever the variation in terminology, the goal of covert action remains constant: to influence events overseas secretly and in support of American foreign policy.

Covert action operations are often grouped according to four broad categories: propaganda, political, economic, and paramilitary (PM) activities. An example of a propaganda operation was the CIA's use of Radio Free Europe during the Cold War to transmit anti-communist themes into nations behind the Iron Curtain. A political CA during the Cold War was the CIA's clandestine funneling of funds to the anti-communist Christian Democratic Party in Italy. An economic example: the CIA attempted to destroy electric power stations in Nicaragua during the 1980s, as a means of undermining the Marxist-oriented S*andinista* regime. PM operations can including everything from assassination plots against foreign heads of state to arming and guiding pro-American insurgent armies in one country or another. Little wonder this has been a controversial subject.

Gregory F. Treverton introduces the reader to covert action in the first chapter of Volume 3. He is followed by Kevin A. O'Brien and Ephraim Kahana, who discuss the use of covert action by other nations. The next four chapters illuminate certain aspects of CA, with James M. Scott and Jerel A. Rosati providing an overview of CA tradecraft (that is, the tools used to implement such operations); Michael A. Turner evaluating the merits of CIA covert propaganda operations; William J. Daugherty looking at political and economic examples of covert action; Jennifer D. Kibbe exploring the entry of the Defense Department into this domain; and former diplomat John D. Stempel contrasting the uses of covert action to diplomatic initiatives. Winding up the volume is Judge James E. Baker's legal analysis of covert action.

Supporting documents include excerpts from the Church Committee Report on the evolution of covert action as carried out by the CIA (Appendix A). The supervision of covert action went from an informal to a highly formal process, as a result of a law known as the Hughes-Ryan Act, passed on December 31, 1974. The language of this statute is presented in Appendix B, and the covert action procedures that resulted from the law are outlined in Appendix C. At the center of the covert action decision process since the Hughes-Ryan Act is the *finding*, a term of art that stems from the passage in the law that requires the president to "find" that a particular covert action proposal is important and has the president's approval. Appendix D contains two findings from the Iran-*contra* era in the mid-1980s. Covert actions must have an organizational apparatus to carry them out, and Appendix E displays what that apparatus looked like during the Cold War (and in basic form remains the organizational chart today, with a few name changes in the boxes).

One of the most controversial forms of covert action has been the assassination of foreign leaders. Appendix F presents a case study from the Church Committee on the CIA assassination plot hatched against the leader of the Republic of Congo, Patrice Lumumba, in 1960. The Committee's exposé of this and other plots led President Gerald R. Ford to sign an executive order prohibiting assassination as an instrument of American foreign policy (see Appendix G). The executive order has been waived in times of authorized warfare against other nations, however, leading to failed attempts to assassinate Saddam Hussein in the first and second Persian Gulf Wars (he was eventually captured alive in 2004, hidden away in a hole near his hometown in Iraq) and Al Qaeda leader Osama bin Laden during the Clinton administration. Considerable ambiguity exists regarding the current status of the executive order and under what conditions it might be waived by administrations. Finally, Appendix H—drawing on a presidential commission study and congressional hearings—examines covert action at its lowest state: the Iran-*contra* affair of the 1980s, when this approach to foreign policy subverted the U.S. Constitution and several laws (including the Hughes-Ryan Act).

A third intelligence mission, after collection-and-analysis and covert action, is counterintelligence (CI) and its associated activity, counterterrorism (CT).

Here is the concentration in Volume 4, titled *Counterintelligence and Counterterrorism: Defending the Nation Against Hostile Forces*. Like covert action, CI went without specific mention in the National Security Act of 1947. By the early 1950s, however, it had similarly achieved a status of considerable importance as an intelligence mission. CI specialists soon waged nothing less than a secret war against antagonistic intelligence services (especially the Soviet KGB); and, after the Cold War, CT specialists would focus on efforts to block terrorists who targeted the United States and its allies. Explaining why the mission of counterintelligence/counterterrorism evolved, a CI expert has pointed out that "in the absence of an effective U.S. counterintelligence program, [adversaries of democracy] function in what is largely a benign environment."[6]

The practice of counterintelligence consists of two matching halves: security and counterespionage. Security is the passive or defensive side of CI, involving such devices as background investigations, fences, sentries, alarms, badges, watchdogs, and polygraphs (lie detection machines). Counterespionage (CE) is the offensive or aggressive side of CI. The most effective CE operation is the infiltration of an American agent or "mole" into the enemy camp, whether a hostile intelligence service or a terrorist cell—a ploy called a penetration. Thus, the practice of security is, according to one of America's top counterintelligence experts, "All that concerns perimeter defense, badges, knowing everything you have to know about your own people," whereas the CE side "involves knowing all about intelligence services—hostile intelligence services: their people, their installations, their methods, and their operations."[7]

Stan A. Taylor and Nigel West clarify these issues in the first two chapters of this volume, then in the next two chapters Katherine A. S. Sibley and Athan Theoharis examine the challenges of keeping the United States spy-free. Rhodri Jeffreys-Jones looks at the efforts in Europe to create a counterintelligence capability similar to that practiced by America's Federal Bureau of Investigation (FBI). Glenn Hastedt takes the reader into the counterterrorism thicket in Washington, DC, explaining how politics influences CI and CT operations. Richard L. Russell and Jennifer Sims discuss the ups and downs of trying to establish an effective counterterrorism response in the United States, complicated by the fragmentation of authority and widely differing cultures among the sixteen U.S. intelligence agencies. Finally, Katharina von Knop looks at the rising role of women in terrorist organizations.

The back-of-the-book documents in Volume 4 begin with a look at the Church Committee findings regarding counterintelligence in 1975 (Appendix A), followed by the notorious Huston Plan—a master counterintelligence spy plan drafted by White House aide Tom Charles Huston in 1970, in response to a nation at unrest over the war in Vietnam (Appendix B). The Huston Plan is a classic illustration of overreaction in a time of domestic strife. In Appendix C, the Senate Select Committee on Intelligence summarizes its findings about the Aldrich H. Ames counterintelligence disaster. Next the appendixes include a series of U.S. commission conclusions about how to improve intelligence in the struggle

against global terrorism, whether locating and penetrating their cells in advance of a terrorist attack or thwarting the ability of terrorists to acquire WMDs. The panel reports include: the Hart-Rudman Commission of 2001 (Appendix D); the 9/11 or Kean Commission of 2004 (Appendix E); and the Silberman-Robb Commission of 2005 (Appendix F). For purposes of comparison, the final appendix (G) examines the conclusions reached by a British commission that also probed the Iraqi WMD failure: the Butler Report of 2004.

The fifth volume in the series, titled *Intelligence and Accountability: Safeguards Against the Abuse of Secret Power*, stems from a concern that secret power might be misused by those in high office. This danger was underscored in 1975 when Congress found the U.S. intelligence agencies guilty of spying against law-abiding American citizens, and again in 1987 during the Iran-*contra* affair when some elements of the intelligence community violated the public trust by ignoring intelligence laws. The United States has been one of the few nations in the world to conduct an ongoing experiment in bringing democratic accountability to secret government activities. Democracy and spying don't mix well. Secrecy runs counter to democratic openness, while at the same time openness possesses a threat to the success of espionage operations. Democracies need intelligence agencies to acquire information that may protect them, but thoughtful citizens worry about having secret agencies in an open society.

Until 1975, the nation's remedy for the tension between intelligence gathering and democracy was to trust the intelligence agencies and hope for the best. Elected officials treated the secret services as exceptional organizations, immune from the checks and balances envisioned by the framers of the Constitution. Lawmakers were satisfied with this arrangement, because if an operation went awry they could duck responsibility. When James R. Schlesinger, DCI in 1973, attempted to inform John Stennis (D-MS), a key member of the Senate Armed Services Committee, about an approaching operation, the Senator stopped him short: "No, no, my boy, don't tell me. Just go ahead and do it, but I don't want to know."[8]

This attitude on Capitol Hill—overlook rather than oversight—underwent a dramatic turnabout in December 1974, however, when the *New York Times* reported on allegations of CIA spying at home and questionable covert actions in Chile. Congress might have waved aside the revelations about Chile as just another Cold War necessity in the struggle against regimes leaning toward Moscow, but spying on American citizens—voters—was another matter altogether. In January 1975, President Ford created the Commission on CIA Activities Within the United States (the Rockefeller Commission, led by his vice president, Nelson Rockefeller). Later that month the Senate established a select committee to investigate intelligence activities. The committee was headed by Frank Church, D-ID, and became known as the Church Committee (the editor served as Church's assistant). A counterpart House committee, led by Representative Otis Pike (D-NY), began investigations the following month.

These various panels, especially the Church Committee, found many more improprieties than they had expected. Not only had the CIA engaged in domestic

spying in violation of its charter, so had the FBI and several military intelligence units. Furthermore, the FBI had carried out secret operations, known collectively as COINTELPRO, against thousands of civil rights activists, members of the Ku Klux Klan, and Vietnam War dissenters. The objective was to make their lives miserable by disrupting their marriages and employment. The Bureau even attempted to blackmail Dr. Martin Luther King Jr. into committing suicide. Church Committee investigators also discovered CIA assassination plots against foreign leaders and efforts to topple President Salvador Allende of Chile, even though he had been democratically elected.

These revelations convinced lawmakers that the time had come to bring accountability into the dark recesses of government. Congress established intelligence oversight committees in both chambers—the Senate in 1976 and the House a year later—and, by 1980, required by law timely reports on all secret intelligence operations. The new Committees pored over intelligence budgets, held regular hearings (mostly in closed session to protect spy sources and methods) and seriously examined the performance of America's intelligence agencies. No other nation has ever so thoroughly applied democratic principles to its secret services, although a number are now beginning to follow the leadership of the United States toward greater intelligence supervision.[9]

Since 1975, this effort has evolved in fits and starts. Sometimes lawmakers have insisted on close accountability, as when they enacted the Intelligence Oversight Act of 1980 with its stringent reporting requirements for covert operations, or when a series of laws in the 1980s sought to end covert actions in Nicaragua. At other times, members of Congress have loosened the reins—for example, repealing in 1985 a prohibition against covert action in Angola. On still other occasions, Congress has concentrated on helping the intelligence agencies improve their security and performance, as with a law in 1982 that prohibited exposing the names of undercover officers. The Iran-*contra* scandal of 1987 was a major setback to this new oversight, as the Reagan administration bypassed most of these rules and statutes in its conduct of a covert war in Nicaragua against the will of Congress. The scandal was an alert to lawmakers. The Intelligence Oversight Act of 1991 further tightened intelligence supervision by clarifying reporting requirements. Lawmakers also set up an Office of Inspector General in the CIA, confirmed by and accountable to Congress.

The pulling and tugging has continued, most recently over whether President George W. Bush violated the Foreign Intelligence Surveillance Act (FISA) of 1978 by conducting warrantless wiretaps as part of the war against terrorism in the aftermath of the 9/11 attacks. The FISA required warrants, but the White House claimed (when the secret operation leaked to the media) the law had become to cumbersome and, besides, the president had inherit authority to conduct the war against terrorism as he saw fit. This debate aside for the moment (several authors address the issue in these volumes), one thing is certain: the intelligence agencies in the United States are now very much a part of the nation's system of checks and balances. Americans want and deserve both civil liberties and a secure defense

against threats; so the search continues for an appropriate balance between liberty and security, democracy and effectiveness—precisely the topic of Volume 5.

The set of chapters on intelligence accountability are introduced with a chapter by David M. Barrett, the foremost authority on the history of accountability in the early years of modern U.S. intelligence (1947 to 1963). The chief counsel of the Church Committee, Frederick A. O. Schwarz Jr., then reflects back on the effects of that watershed inquiry. Next, the editor offers a previously unpublished interview with DCI William E. Colby, who stood at the helm of the intelligence community as it weathered the storm of the investigations into domestic spying during 1975. Mark Phythian presents a chapter on the British experience with intelligence accountability; and, comparing British and American oversight, Lawrence J. Lamanna contrasts the responses on both sides of the Atlantic to the faulty Iraqi WMD assessments in 2002.

The next chapter, written by Cynthia M. Nolan, looks at contemporary issues of intelligence oversight in the United States. Hans Born and Ian Leigh follow with a comparative dimension by contrasting intelligence accountability practices in a variety other nations. Finally, A. Denis Clift and Harry Howe Ransom, who have witnessed the unfolding of intelligence accountability over the past four decades, offer their appraisals of where the experiment stands today.

The first supporting document in this volume is a succinct legislative history of intelligence accountability from 1947 to 1993, prepared by the Senate Select Committee on Intelligence (Appendix A). Then come a series of important oversight laws, beginning with FISA in 1978. With this law, members of Congress sought to rein in the open-ended authority of the executive branch to wiretap and otherwise spy on individuals considered risks to the national security—a privilege abused by a number of administrations from the 1930s forward. Henceforth, FISA required a warrant from a special court (the FISA Court, whose members are appointed by the Chief Justice of the Supreme Court) before such intrusive measures could be carried out. This law, a hot topic in 2005–6 when critics charged the second Bush administration with violation of the warrant requirement, can be found in Appendix B.

The Intelligence Oversight Act of 1980 is presented in Appendix C. This is a brief but nonetheless far-reaching law, enacted by Congress as an attempt to become an equal partner with the executive branch when it came to intelligence. The 1991 Intelligence Oversight Act (Appendix D) emerged after the Iran-*contra* scandal and provided a tightening and clarification of the language in its 1980 precursor, especially with respect to the approval and reporting rules for covert action. The political tug-of-war over the drafting of this currently prevailing oversight statute was intense, leading to the first and only presidential veto of an intelligence act. President George H. W. Bush found the proposal's insistence on prior reporting of covert action objectionable in times of emergency. Lawmakers entered into a compromise with the chief executive, settling on a two-day reporting delay in emergencies. The bill passed Congress again, this time without a presidential veto.

In 1995, the House Permanent Select Committee on Intelligence launched an inquiry into a wide assortment of intelligence issues, stimulated initially by counterintelligence concerns (Aldrich Ames's treasonous activities at the CIA had recently been discovered) but turning into an opportunity for a broad review of new challenges that faced the secret agencies now that the Cold War had ended. In Appendix E, an excerpt from the Committee's final report examines the state of intelligence accountability in the mid-1990s. The next document, in Appendix F, carries the examination into the twenty-first century, with the appraisal of the 9/11 Commission on the same subject. The commissioners were unimpressed, referring to intelligence accountability as "dysfunctional."

At the center of any efforts to maintain accountability for the secret agencies lies the question of funding—the mighty power of the pursue, held in the hands of lawmakers. Appendix G draws on the findings of the Aspin-Brown Commission to provide official documentation about how the United States spends money for spying. Finally, in Appendix H, DCI Robert M. Gates (1991–93) offers observations about oversight from the perspective of the intelligence community management team, located at that time on the Seventh Floor of the CIA.

Here, then, is what the reader will find in these five volumes. The editor and the contributors hope the chapters and documents will help educate the public about the importance of intelligence agencies, as well as stimulate scholars around the world to further the blossoming of this vital field of study. I am pleased to acknowledge my gratitude to Praeger's Heather Staines, senior project editor, and Anne Rehill, development editor, each a pleasure to work with and most helpful in their guidance; Julie Maynard at the University of Georgia for her administrative assistance; Lawrence J. Lamanna, my graduate research assistant, for his good counsel and logistical help; Leena S. Johnson for her indispensable encouragement and support; and the contributors to these volumes for their outstanding scholarship and their much appreciated cooperation in keeping the publishing train running on time.

These volumes are enthusiastically dedicated to Harry Howe Ransom, who has done so much in the United States to lead the way toward a serious discipline of intelligence studies.

Loch K. Johnson

NOTES

1. Some of the authors have had multiple careers, so in categorizing them I have counted the place where they have spent most of their professional lives.

2. Quoted by Senator Frank Church (D-ID), in *Congressional Record* (January 27, 1976), p. 1165.

3. *Fact Book on Intelligence* (Washington DC: CIA Office of Public Affairs, April 1983), p. 17.

4. National Security Act of 1947, signed on July 26, 1947 (P.L. 97-222; 50 U.S.C. 403, Sec. 102).

5. Comment, "Evening News," NBC (January 13, 1978).

6. Editor's interview with a FBI counterintelligence specialist, Washington, DC (May 16, 1975).

7. Editor's interview with Raymond Rocca, CIA/CI specialist, Washington, DC (November 23, 1975).

8. Editor's interview with James R. Schlesinger, Washington, DC (June 16, 1994).

9. See Hans Born, Loch K. Johnson, and Ian Leigh, *Who's Watching the Spies? Establishing Intelligence Service Accountability* (Washington, DC: Potomac Books, 2005).

1

AN INTRODUCTION TO THE INTELLIGENCE STUDIES LITERATURE

LOCH K. JOHNSON

BEFORE THE "YEAR OF INTELLIGENCE"

IN 1975, PROFESSOR HARRY HOWE RANSOM OF Vanderbilt University, a top intelligence researcher and a pioneer in the field, noted that he had been going after the subject with a pick and shovel for years, when—all of a sudden—various government investigative panels began to use bulldozers to unearth a mountain of new information.[1] He was referring to the inquiries conducted by the Church Committee in the U.S. Senate (led by Frank Church, D, Idaho), the Pike Committee in the U.S. House (led by Otis Pike, D, New York), and the Rockefeller Commission in the Ford White House (led by Vice President Nelson Rockefeller), all stimulated by *New York Time*s revelations that the Central Intelligence Agency (CIA) had spied on American citizens over the past decade.[2] These investigative panels had indeed added significantly to the extant literature on America's secret agencies, with the reports from the Church Committee alone rising in a stack some five-feet high.[3]

This "Year of Intelligence" (1975, less affectionately known by some intelligence officers as the "Intelligence Wars") did represent a watershed in a number of ways. For example, before 1975 the Congress permitted the CIA and its sister agencies in the "intelligence community" to carry out operations at home and abroad without much legislative supervision. The allegations by the *New York Times* of domestic spying changed all that, as lawmakers scurried to prevent future intelligence abuses and allay the fears of folks back home (voters) that the CIA had become an American gestapo. The government of the United States began its ongoing experiment in intelligence accountability, now widely emulated in countries around the world.[4] The goal was to seek a better balance between

security concerns, on the one hand, which require the existence of efficient intelligence agencies, and liberty, on the other hand, which rests upon safeguards against the abuse of secret power.

The year 1975 was a watershed in another sense, too, related to the extent of research documents and studies available on intelligence. As Professor Ransom's comment suggests, before this *annis mirabilis* the intelligence studies cupboard was, if not bare, then scantily stocked.[5] The most noteworthy efforts since the creation of the modern American intelligence system after World War II came from Sherman Kent, a Yale University history professor known for his keen intellect and salty tongue, and who would later become an important organizing force inside the CIA for the development of its analytic capabilities; from Lyman B. Kirkpatrick Jr., another CIA official; from Professor Ransom, a professor at Harvard University when he first became interested in intelligence studies and who did much to inform the general public as well as scholars about intelligence in those early years; from Roger Hilsman, a government official and political scientist; and from journalists David Kahn and David Wise.[6]

Other significant works consisted chiefly of memoirs and biographies of various spies and spymasters,[7] along with examinations of intelligence successes and failures,[8] the difficulties of disseminating intelligence to busy and sometimes blinkered policy officials,[9] studies of Soviet intelligence operations against the United States,[10] exposés (of uneven reliability),[11] sporadic academic books or scholarly journal articles in the spirit of Kent and Ransom,[12] the rare textbook that devoted serious attention to the subject,[13] and the occasional newspaper article providing an in-depth look into one of the secret agencies.[14]

Both before and after 1975, much of the literature on intelligence has been speculative, unreliable, and sometimes wholly without merit; the reader and researcher have to be especially wary about books and articles claiming to understand the secret machinations of government agencies hidden behind guarded buildings and barbed-wire fences, not to mention multiple veils of classification. Since 1975, though, the availability of reliable documentation and research findings on intelligence has expanded dramatically—one could say exploded—and this chapter outlines some (but by no means all) of the notable features of this new research terrain.

AFTER THE "YEAR OF INTELLIGENCE"

The literature on intelligence in 1975 is vast and difficult to capture in a short chapter, even one that concentrates only on the literature in English. Indeed, this bibliography should be viewed more as a sampler than any effort to be comprehensive; many a good work will not be mentioned because of space limitations, and the reader is encouraged to consult literature reviews of greater length.[15] The objective here is simply to give the reader a sense of the chief topics and some of the major works that have addressed them.

On top of a stunning proliferation of books and articles on intelligence since the watershed year, the field has also witnessed the emergence of credible scholarly journals dedicated to intelligence studies.[16] To facilitate an examination of this literature, this chapter groups an array of studies into the following four broad categories: intelligence history, structure, and theory; intelligence missions (collection-and-analysis, counterintelligence, and covert action); intelligence accountability, ethics, and reform; and intelligence leadership and management.

Intelligence History, Structure, and Theory

British scholars have been particularly adept at offering insightful histories of intelligence within both the United Kingdom and the United States, as well as for other countries. The leaders have been the Cambridge University historian Christopher Andrew and King's College, London, professor Lawrence Freedman,[17] but they have enjoyed good company with Aldrich;[18] Cradock, who provides a practitioner's point of view;[19] Davies;[20] Foot;[21] Hennessy;[22] Jackson;[23] Jeffreys-Jones;[24] Ranelagh, who has written the most comprehensive history of the CIA;[25] Shukman;[26] Stevenson;[27] and West.[28]

American, Canadian, and German scholars have provided useful intelligence histories, too. Samples include, on the U.S. side, works by Corson,[29] Gaddis,[30] Handel,[31] Leary,[32] May,[33] Naftali,[34] Richelson,[35] Rudgers,[36] Smith,[37] Troy,[38] Warner,[39] Winks,[40] and Zegart;[41] on the Canadian side, Charters and Ferris,[42] as well as Farson, Stafford, and Wark;[43] and on the German side, Krieger.[44] Two government reports contain reliable histories of the CIA, prepared by Karalekas and by McNeil;[45] and, for histories of one of the most traumatic years in American intelligence (1975), see Johnson and Smist.[46]

Organizational blueprints ("wiring diagrams") usually fail to reveal much about how intelligence organizations actually function, but they are a starting point. With respect to the United States, Lowenthal and Richelson have laid out the connections among America's sixteen intelligence agencies[47]—although new intelligence managers are inclined to change the names of various component parts, which makes the writing on this aspect of intelligence highly perishable. Cline, a particularly thoughtful senior intelligence official, traced the evolution of the CIA from 1947 to 1981;[48] Hastedt and Zegart examined organizational influences on intelligence failures;[49] and Andrew published studies on the organization of British and of Soviet intelligence.[50] A significant structural question is the relationship between the intelligence services of different nations. In one important example of research in this area, Richelson and Ball have explored ties between the United Kingdom and the United States.[51]

Theories have been difficult to construct in the intelligence field because the empirical data base for constructing and testing theories still remains relatively thin. Nonetheless, a number of scholars have made tentative forays into this uncertain terrain. Illustrations include the work of Betts,[52] Davies,[53] Handel,[54]

Herman,[55] Hulnick,[56] Loch K. Johnson,[57] Rob Johnson,[58] Kahn,[59] Laqueur,[60] Robertson,[61] Shulsky,[62] and a special issue of *Intelligence and National Security* edited by Len Scott and Peter Jackson.[63] The question of transparency, the flipside of secrecy, is addressed by Lord and Finel.[64] Overall, the studies on intelligence theory find that the discipline remains in its infancy, holding great promise for scholars interested in blazing new trails.[65]

Intelligence Missions

Intelligence may be sorted into three primary missions: the collection and interpretation ("analysis") of information; the protection of government secrets against hostile intelligence services and other threats ("counterintelligence"); and the clandestine manipulation of events in foreign lands on behalf of a nation's interests, through the use of propaganda, political activities, economic disruption, and paramilitary operations (collectively known in the United States as "covert action" or "special activities"). Each of these missions has attracted the attention of intelligence scholars, especially collection, analysis, and dissemination—the heart and soul of intelligence.

Collection, Analysis, and Dissemination

The collection of intelligence relies on technical means (satellites and reconnaissance airplanes, for example—so-called technical intelligence or TECHINT, in the professional acronym); on human means (classic espionage or human intelligence—HUMINT); and on the sifting of information available in the open literature (newspapers, public speeches, and the like—sometimes referred to as open-source intelligence or OSINT). In the U.S. experience, many of the best contributions from spy machines have come from relatively inexpensive unmanned aerial vehicles (UAVs), notably the *Predator*, which in 2003–06 proved effective for scouring the Iraqi and Afghani countryside in search of insurgents. On occasion, far more costly surveillance satellites have demonstrated their value, too, by intercepting revealing telephone conversations among terrorists and other enemies (a method known as "signals intelligence" or SIGINT, a term for describing the capture of communications from one person or group to another).

Moreover, satellite photographic images of Russian and Chinese missile sites, or North Korean troop movements, continue to be valuable for the security of the United States. Still, in the case of terrorism, it would be more advantageous to have a human agent well placed inside the upper reaches of the Al Qaeda organization; such an agent ("asset") would be worth a dozen multibillion-dollar satellites.

Aim, Bamford, Kahn, and Keefe have examined the arcane technology of SIGINT in the United States;[66] Burrows writes on space surveillance;[67] and Richelson offers insights into a broad range of TECHINT developments in U.S. intelligence.[68] While chronicling its successes and failures since 1947, Hitz spells out many of the key dilemmas in America's practice of HUMINT;[69] and Gerecht

provides a persuasive critique that the United States has ignored the use of non-official cover (NOC) for HUMINT operational officers overseas, thereby missing many opportunities to understand foreign societies by having personnel out in the field rather than inside U.S. embassies.[70] In the United States, a leading guru on OSINT has been Robert David Steele.[71]

At the core of intelligence is the challenge of analysis. Here the goal is to bring insight to the information that has been collected and processed. The method is straightforward: hire smart people to sift through all the information available in an attempt to predict what events may happen next in the world. Jervis has published influential research about the difficulties of carrying out analysis.[72] So has his colleague at Columbia University, Betts, who cautions—in one of the most widely read pieces on intelligence analysis—that when it comes to predicting events in the world, one must develop a "tolerance for disaster."[73] A CIA analyst, Jack Davis, has explored the policy maker's perspective on the analytic process in an in-depth interview of a key U.S. ambassador and recipient of many intelligence reports over the years;[74] Knorr has authored a case study of CIA analysis prior to the Cuban missile crisis in 1962;[75] Kahana, another case study, on the Yom Kippur War of 1973 (from the Israeli perspective);[76] Prados, a study on U.S. intelligence assessments of the Soviet Union;[77] and Russell, a report on the performance of intelligence analysts before and during the first Persian Gulf War.[78] For an exploration of unconventional analytic topics that have come before the U.S. intelligence agencies in the aftermath of the Cold War (for example, environmental and global health intelligence), see Johnson.[79]

Once information is analyzed, it is ready to be passed along to policy officials. This task is known as dissemination. Perhaps the greatest paradox of intelligence is that so much effort and funding go into the gathering of information for policy makers, only to have them ignore it. Some of the best assistant secretaries of defense and state have conceded that they spent, at best, five minutes a day scanning intelligence reports; they were simply too overwhelmed with other obligations. These pressures would be even more constraining for men and women higher up the policy hierarchy. The first challenge of dissemination, then, is to catch the attention of busy leaders, and this is why the marketing of intelligence is critical.

In marketing their products to consumers, the secret agencies confront several potential obstacles. Policy makers may choose to twist ("cook" or "spin") intelligence to fit their own political views or ideological predispositions, a distortion of information known as "politicization." Intelligence officers themselves may succumb to the temptation to slant information to suit the needs of policy makers, as a way of advancing their careers by attracting favorable attention from powerful political figures—a phenomenon known as "intelligence to please." Fortunately, this temptation on the analyst's side of the equation occurs infrequently, because most analysts are imbued with a sense of professional ethics that shuns the practice of twisting information to please politicians.

More common is politicization on the consumer side: policy makers bending the facts to support policy objectives. Speaking truth to power is a notoriously difficult endeavor. Those in power often do not want to hear information that runs counter to their policy preferences; hence, they sometimes distort intelligence reports. An illustration is "cherry-picking," whereby decision makers select from intelligence reports only those snippets of information and analysis that uphold their stated policy positions, ignoring countervailing facts or conclusions.

Some government officials have been known to dismiss entire intelligence reports, as President Lyndon B. Johnson did with CIA analyses that came to a dismal prognosis about the likelihood of U.S. military victory in the Vietnam War; or as the second Bush administration did with CIA reports that found no connections between Al Qaeda and Saddam's regime in Iraq. In such instances, the unenviable but vital responsibility of intelligence managers is to call policy officials to account for their distortions, publicly if necessary.

Writings by Lowenthal,[80] Ransom,[81] and Wirtz[82] reveal the importance of understanding the issues of intelligence dissemination. They point to the need to maintain a high wall between policy officials and intelligence officers. Such a wall is necessary not in the sense of preventing communications between the two groups about intelligence collection and analysis priorities, which is important; but, rather, to curb political ties between the two groups and the twisting of intelligence to meet policy objectives. The need for a wall notwithstanding, there is a sense among intelligence scholars that intelligence officers and law enforcement officials do need to reach out to each other and work together more closely in protecting the United States against security threats.[83]

Exploring still another angle of consumer-producer relations, Hastedt has written on the question of "public intelligence"—how intelligence goes beyond the narrow consumer-producer domain to enter the realm of public discussion.[84]

Counterintelligence

Protecting a nation's secrets—everything from the names of agents overseas to the methods used for spying on others—is the domain of counterintelligence. Some of the leading research here focuses on failures to stop the infiltration of "moles" into one's own intelligence services. For example, the journalist David Wise has devoted much of his professional career to the preparation of case studies on American moles, most recently the CIA traitor Aldrich H. Ames and the Federal Bureau of Investigation (FBI) traitor Robert Hanssen.[85]

A British writer, Tom Mangold, offers the most thorough study to date of America's premier spy catcher during the Cold War, James J. Angleton, Chief of Counterintelligence at the CIA from 1954 to 1974.[86] Taylor and Snow examine more broadly the questions of why intelligence officers become traitors and how they are uncovered;[87] Peake looks at counterintelligence and the Office of Strategic Services (OSS), exploring the extent to which the United States was infiltrated by Soviet spies during World War II;[88] Sibley explores the presence of

communist spies inside the United States at the beginning of the Cold War;[89] and West brings together a valuable overview on the subject of spy catching.[90]

A subset of the counterintelligence literature is comprised of studies on counterterrorism. This field is vast and growing exponentially since the attacks of September 11, 2001. Another survey like this one could be prepared for the counterterrorism literature alone, but for starters, see Cole and Dempsey; Gressang; and Von Knop, Neisser, and Van Creveld; and Shultz and Dew.[91]

Covert Action

Covert action may be defined as those activities carried out by the CIA to secretly influence and manipulate events abroad. This approach is often referred to as the "Third Option"—in between sending in the Marines, on the one hand, and relying on the diplomatic corps to achieve one's goals, on the other hand. The use of military force is "noisy" and likely to draw a quick reaction from adversaries, as well as stir widespread debate at home; and diplomacy can be notoriously slow and often ineffectual. Thus, covert action has had a special appeal to some presidents and their aides. With this tool, they can move rapidly and in relative quiet, avoiding lengthy public discussions over tactics and broader objectives (hence, the "quiet option" is another euphemism for covert action).

In the United States, covert action has often failed, as with the Bay of Pigs operation against Cuba in 1961 and the Iran-*contra* scandal in 1986. The latter especially discredited covert action, because the Reagan administration carried out CIA paramilitary operations against Nicaragua despite strong congressional opposition and a law preventing such activities in that Central American nation. After the Iran-*contra* episode, the budget for covert action plummeted to its lowest levels: less than 1 percent of the CIA's annual budget. It would take the terrorist attacks against the United States on September 11, 2001, to stimulate a renewed interest in this approach to secret foreign policy. After 9/11, funding for covert action began a rapid rise upward in the name of combating world terrorism. In 2001–2, the use of CIA paramilitary operations against the Taliban regime in Afghanistan, in tandem with overt military operations by the indigenous Northern Alliance and U.S. bombing missions, opened a new—and, in this case, quite successful—chapter in America's reliance on paramilitary covert actions.

Covert action is particularly hard to research, because most of the archives on this subject remain locked up in the vaults of the CIA. Nevertheless, in the United States, scholars have been able to ferret out enough information to provide a fairly good sense of this super-secret domain. Among the leading researchers are Coll,[92] Daugherty,[93] Godson,[94] Immerman,[95] Johnson,[96] Knott,[97] O'Brien,[98] Prados,[99] Reisman and Baker,[100] Treverton,[101] Weissman,[102] and Wyden (on the Bay of Pigs fiasco).[103] Valuable, too, are the hearings and reports of the Church Committee, published in 1975 and 1976,[104] as well as revealing case studies of covert action in Iran and in Guatemala, written respectively by Roosevelt and by Wise and Ross.[105] Overviews by CIA insiders can be found in Baer, Scheuer,

Rositzke, and Shackley;[106] and journalist Bob Woodward has given his impressions of the CIA and covert action during in the Reagan years.[107] Two prominent members of Congress have recalled their experiences during the Iran-*contra* investigation into covert action in Nicaragua.[108] And on the relationship between CIA covert action and military special operations, see Kibbe.[109]

Accountability, Ethics, and Reform

In democracies, there is a belief that even secret agencies—perhaps most especially secret agencies—ought to be held responsible for their actions, as an important check on possible abuses of power. The means by which they are held responsible is known as accountability or "oversight"—the review of executive branch programs by lawmakers, judges, inspectors general, and special investigative panels. The literature in this subfield of intelligence studies is growing, just as in all the other subfields. In the United States, among the chief examples are Barrett (covering the early years of the Cold War),[110] Hitz,[111] Johnson,[112] Kaiser,[113] Koh,[114] Olmsted,[115] Oseth,[116] and Treverton;[117] and, with special attention to the question of civil liberties, Commager,[118] Donner,[119] Elliff,[120] Morgan,[121] Schwarz,[122] Theoharis,[123] and Wise.[124] Manget has explored the neglected topic of judicial oversight in the United States.[125] On intelligence oversight in the United Kingdom, Gill and Phythian have been leading researchers.[126] And Whitaker examines the threat to individual liberty and privacy posed by growing government surveillance in modern societies.[127] Recently, scholars studying accountability have tried to incorporate a systematic comparative dimension into their work, contrasting the systems of oversight in different countries (see Born, Johnson, and Leigh[128]).

The overall conclusion reached by most studies on intelligence accountability is that oversight in often overlooked by lawmakers, who perceive few incentives for laboring behind closed doors to review intelligence programs when their re-election depends on a more public display of legislative activity.[129] The unfortunate end result of this inattention is an absence of checks on the secret agencies, which can result in intelligence failures like 9/11 and the Iraqi weapons of mass destruction (WMD), scandals like the CIA/FBI domestic spying finally revealed by the media and Congress in 1974–75, and the Iran-*contra* affair disclosed in 1986.

Less researched is the ethical dimensions of intelligence—an oxymoron for some who believe that no bright lines should exist between the safety of a nation and the gathering of intelligence or the use of covert action to advance national interests. Among the most thoughtful offerings in this area have been from Barry, Godfrey, and Herman, each of whom demonstrates that bright lines do, and should, exist for intelligence (just as with a nation's war-making powers).[130]

Intelligence reform has long been a topic of interest to scholars and citizens alike. Since the CIA was established in 1947, the reform literature in the United

States has steadily commented on the need to improve various aspects of American intelligence. These commentaries have usually been in the form of reports from numerous congressional investigative panels and presidential commissions through the years that have dealt with intelligence issues.[131] Beyond these official government critiques are several analyses by U.S. scholars, many stimulated by the tragic 9/11 intelligence failure.[132]

The conclusion reached by most of these studies is that the United States needs a strong Director of National Intelligence (DNI), not the weak one yielded by legislation in December 2004 (the Intelligence Reform and Terrorism Prevention Act); and that America's intelligence agencies must work together more closely to share information about threats facing the United States, eschewing their cultural proclivities toward parochialism. In a phrase, intelligence consolidation must replace the current dispersal of authority.

Intelligence Leadership and Management

As the consensus view on the need for stronger leadership for the U.S. intelligence "community" suggests, scholars and reformers alike see leadership and management as important dimensions of intelligence. A few scholarly studies exist on this topic.[133] By and large, though, the most insightful explorations of intelligence leadership and management have come from the experiences of the individuals who have led the intelligence agencies—memoirs by America's Directors of Central Intelligence (DCIs, the title of the nation's intelligence chief from 1947 until the 2004 law that replaced this office with a DNI) or other key officials in the world of espionage.[134] One portrait that emerges from these insider accounts is of a secret world where intelligence bureaucrats enjoy considerable discretionary powers, with intelligence managers finding it difficult to rein in the offices and bureaus beneath them in the organizational hierarchy. The classic case is the Operations Directorate in the CIA—notoriously resistant to supervision by managers on the Agency's Seventh Floor.[135]

An important aspect of intelligence management is the question of government secrecy. Reformists have written extensively about the excessive use of secrecy in the United States, which they consider anathema to the fundamental principles of a democratic, open society.[136]

THE FUTURE RESEARCH AGENDA

As this bibliographic chapter indicates, the field of intelligence studies is broad. Unfortunately, from the point of view of trying to understand how to make intelligence less prone to failure, it is also shallow—a fact reflective of the field's relative infancy. Or perhaps from another vantage point, one could say the shallowness is fortunate, at least for scholars who may be interested in the challenge of

helping to establish a new field of study. Every single category presented here awaits the energy, hard work, and insight of scholars. Much good work has been done by the pioneers of intelligence studies, but much remains to be done.

NOTES

1. Comment to the author, Washington, DC (December 20, 1975).

2. See J. Leiper Freeman, "Investigating the Executive Intelligence: The Fate of the Pike Committee," *Capitol Studies* (Fall 1977), pp. 103–17; Loch K. Johnson, *Season of Inquiry* (Lexington: University Press of Kentucky, 1985) and "Congressional Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee," *Public Administration Review* 64 (January/February 2004), pp. 3–14; and Frank J. Smist Jr., *Congress Oversees the United States Intelligence Community* (Knoxville: University of Tennessee Press, 1976).

3. For the Church Committee reports, see especially Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Final Report*, 94th Cong., 2d Sess. Sen. Rept. No. 94-755, 6 vols. (Washington, DC: Government Printing Office, 1976), "Alleged Assassination Plots Involving Foreign Leaders," *Interim Report*, S. Rept. No. 94-465 (Washington, DC: Government Printing Office, November 20, 1975), and Anne Karalekas, "History of the Central Intelligence Agency," *Supplementary Detailed Staff Reports on Foreign and Military Intelligence*, S. Rept. No. 94-755, vol. 4 (Washington, DC: Government Printing Office, April 23, 1976), pp. 1–107. The top-secret Pike Committee Report was leaked by a still unknown source and can be found in "The Report on the CIA That President Ford Doesn't Want You to Read," *Village Voice* 21 (1976). For the Rockefeller Commission Report, see Commission on CIA Activities within the United States, *Report to the President* (Washington, DC: Government Printing Office, June 1975).

4. Hans Born, Loch K. Johnson, and Ian Leigh, eds., *Who's Watching the Spies? Establishing Intelligence Service Accountability* (Washington, DC: Potomac Books, 2005).

5. This chapter does not address the writing on intelligence from the early master strategists, but their enduring observations on intelligence deserve to be read, e.g., Carl von Clausewitz, *On War*, edited by Anatol Rapoport (New York: Pelican, 1968).

6. Roger Hilsman, *Strategic Intelligence and National Decisions* (Glencoe: Free Press, 1956); David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: Macmillan, 1967); Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press, 1949, revised in 1965), and "Estimates & Influence," *Foreign Service Journal* (April 1969); Lyman B. Kirkpatrick Jr., *The Real CIA* (New York: MacMillian, 1968) and *The U.S. Intelligence Community* (New York: Hill and Wang, 1973); and Harry Howe Ransom, *Central Intelligence and National Security* (Cambridge: Harvard University Press, 1958),"How Intelligent Is Intelligence?" *New York Times Magazine* (May 22, 1960), pp. 20, 77–79, "Secret Mission in an Open Society," *New York Times Magazine* (May 21, 1961), pp. 20, 77–79, *The Intelligence Establishment* (Cambridge, MA: Harvard University Press, 1970), and "Strategic Intelligence and Foreign Policy," *World Politics* 27 (October 1974), pp. 131–46; David Wise

and Thomas Ross, *The Invisible Government* (New York: Random House, 1964); David Wise, *The Espionage Establishment* (New York: Random House, 1967) and *The Politics of Lying* (New York: Random House, 1973). For one of the earliest scholarly studies on U.S. intelligence, see Henry M. Wriston, *Executive Agents in American Foreign Relations* (Baltimore: Johns Hopkins University Press, 1929).

7. Stewart Alsop and Thomas Braden, *Sub Rosa: The OSS and American Espionage* (New York: Reynal and Hitchcock, 1946); Allen Dulles, *The Craft of Intelligence* (Westport, CT: Greenwood, 1977); and Greville M. Wynne, *The Man From Moscow: The Story of Wynne and Penkovsky* (London: Hutchinson, 1967).

8. Anthony Cave Brown, *Bodyguard of Lies* (New York: Harper & Row, 1975), on World War II British intelligence operations; Sir John Masterman, *Double Cross System of the War of 1939–45* (New Haven: Yale University Press, 1972), another look at British intelligence; Seth W. Richardson, "Why Were We Caught Napping at Pearl Harbor?" *Saturday Evening Post* (May 24, 1947), pp. 79–80; and Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962), a study on intelligence with rare theoretical sensitivities.

9. Thomas L. Hughes, "The Power to Speak and the Power to Listen: Reflections in Bureaucratic Politics and a Recommendation on Information Flows," in *Secrecy and Foreign Policy*, edited by Thomas Franck and Edward Weisband (New York: Oxford University Press, 1974).

10. For example, John Barron, *KGB: The Secret Work of Soviet Agents* (Pleasantville, NY: Reader's Digest, 1974).

11. Samuel Adams, "Vietnam Cover-Up: Playing War with Numbers," *Harper's* 250 (May 1975), pp. 41–44, questioning the possible distortion of intelligence reporting from Vietnam; Philip Agee, *Inside the Company: CIA Diary* (Harmondsworth, Eng.: Penguin, 1975), a controversial "outing" of CIA officers and programs by a disgruntled former CIA officer; Richard Blum, ed., *Surveillance and Espionage in a Free Society* (New York: Praeger, 1972); Stuart H. Loory, "The CIA's Use of the Press: 'A Mighty Wurlitzer,' " *Columbia Journalism Review* (September/October 1974), pp. 8–18; Patrick J. McGarvey, *CIA: The Myth and the Madness* (New York: Saturday Review Press, 1972); Victor Marchetti and John D. Marks, *The CIA and the Cult of Intelligence* (New York: Knopf, 1974), a widely read, authoritative, and influential book at the time of its publication, written by two disgruntled former intelligence officers (with Marchetti highly perched in the CIA); Fletcher L. Prouty, *The Secret Team: The CIA and Its Allies in Control of the United States and the World* (Englewood Cliffs, NJ: Prentice Hall, 1973); and Sol Stern, "NSA and the CIA," *Ramparts* 5 (March 1967), pp. 29–38.

12. Gordon B. Baldwin, "Congressional Power to Demand Disclosure of Foreign Intelligence Agreements," *Brooklyn Journal of International Law* 3 (1976), pp. 1–30; Paul W. Blackstock, "The Intelligence Community Under the Nixon Administration," *Armed Forces and Society* 1 (February 1975), pp. 231–51; William J. Barnds, "Intelligence and Foreign Policy: Dilemmas of a Democracy," *Foreign Affairs* 47 (January 1969), pp. 281–95; Lawrence M. Baskir, "Reflections on the Senate Investigation of Army Surveillance," *Indiana Law Journal* 49 (Summer 1974), pp. 618–53; Ray Cline, "Policy Without Intelligence," *Foreign Policy* 17 (Winter 1974–75), pp. 121–35; Chester Cooper, "The CIA and Decisionmaking," *Foreign Affairs* 50 (January 1972), pp. 223–36; Robert F. Ellsworth and Keith L. Adelman, "Foolish Intelligence," *Foreign Policy* 36 (Fall 1971), pp. 147–59; Stanley Levell, *Of Spies and Strategems* (New York: Prentice-Hall,

1963); Richard Harris Smith, *OSS: The Secret History of America's First Central Intelligence Agency* (Berkeley: University of California Press, 1972); Sanford Ungar, *FBI* (Boston: Atlantic Monthly, 1975); Jerrold L. Walden, "The C.I.A.: A Study in the Arrogation of Administrative Powers," *George Washington Law Review* 39 (October 1970), pp. 66–101; and F. W. Winterbotham, *The Ultra Secret* (New York: Dell, 1975).

13. The best example is Richard C. Snyder and Edgar S. Furniss Jr., *American Foreign Policy* (New York: Rhinehart, 1954).

14. For example, Tom Wicker, et al. "C.I.A. Operations: A Plot Scuttled," *New York Times* (April 25, 1966), p. A1.

15. See, for instance, Mark Lowenthal, *The U.S. Intelligence Community: An Annotated Bibliography* (New York: Garland, 1994), as well as his popular text *Intelligence: From Secrets to Policy*, 3rd ed. (Washington, DC: CQ Press, 2003); and the references in Loch K. Johnson and James J. Wirtz, ed., *Strategic Intelligence: Windows Into a Secret World* (Los Angeles: Roxbury, 2004).

16. The key journals in the field are *Intelligence and National Security* and the *International Journal of Intelligence and CounterIntelligence*, both established in the mid-1980s and both currently published by the Taylor & Francis Group in London. Important, too, is a journal published by the CIA's Center for the Study of Intelligence, entitled *Studies in Intelligence*. It is printed in both a classified version for cleared government officials and, with a different set of articles, an unclassified version for the outside reader. The National Military Intelligence Association also publishes, irregularly, a journal called the *American Journal of Intelligence*. The mainstream scholarly journals in history, political science, international affairs, strategy, and public administration will occasionally carry an article on intelligence, but they are rare. The *American Political Science Review*, for example, has only one article on this subject in its entire history dating back to the early 20th century.

17. Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive, vol. 1: The KGB in Europe and the West* (New York: Penguin/Basic Books, 1999); Christopher Andrew, *For the President's Eyes Only: Secret Intelligence and the American Presidency* (London: HarperCollins, 1995); Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story* (London: Hodder & Stoughton, 1990); Christopher Andrew and David Dilks, eds., *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century* (Urbana: University of Illinois Press, 1984). Among Professor Freedman's many works on intelligence are *U.S. Intelligence and the Soviet Strategic Threat* (Princeton: Princeton University Press, 1986) and "The Politics of Warning: Terrorism and Risk Communications," *Intelligence and National Security* 20 (September 2005), pp. 379–438.

18. Richard Aldrich, *The Hidden Hand: Britain, America and Cold War Secret Intelligence* (London: John Murray, 2001).

19. Percy Cradock, *Know Your Enemy: How the Joint Intelligence Committee Saw the World* (London: John Murray, 2002).

20. See, for example, Philip H. J. Davies, "Ideas of Intelligence," *Harvard International Review* (Fall 2002).

21. M. R. D. Foot, *SOE in France* (London: Cass, 2004).

22. Peter Hennessy, *The Secret State: Whitehall and the Cold War* (London: Allen Lane Penguin Press, 2002).

23. See, for example, Peter Jackson, "The Politics of Secret Service in War, Cold War and Imperial Retreat," *Contemporary British History* 14 (2003), pp. 423–31.

24. Rhodri Jeffreys-Jones, *The CIA & American Democracy* (New Haven: Yale University Press, 1989), and *Cloak and Dollar: A History of American Secret Intelligence* (New Haven: Yale University Press, 2002).

25. John Ranelagh, *The Agency: The Rise and Decline of the CIA* (New York: Simon & Schuster, 1986).

26. Harold Shukman, ed., *Agents for Change: Intelligence Services in the 21st Century* (London: St. Ermin's Press, 2000).

27. William Stevenson, *A Man Called Intrepid* (Basingstoke and London: Macmillan, 1976).

28. Nigel West, *MI6: British Secret Intelligence Operations, 1909–45* (London: Weidenfeld & Nicholson, 1983).

29. William R. Corson, *The Armies of Ignorance: The Rise of the American Intelligence Empire* (New York: Dial, 1977).

30. John Lewis Gaddis, "Intelligence, Espionage, and Cold War Origins," *Diplomatic History* 13 (Spring 1989), pp. 191–212. See also: Christopher Andrew, "Intelligence and International Relations in the Early Cold War," *Review of International Studies* 24 (1998).

31. Michael Handel, *War, Strategy and Intelligence* (London: Cass, 1987).

32. William M. Leary, *Perilous Mission: Civil Air Transport and CIA Covert Operations in Asia* (Tuscolusa: University of Alabama Press, 1984).

33. Ernest R. May, ed., *Knowing One's Enemies: Intelligence Assessment Before the Two World Wars* (Princeton: Princeton University Press, 1985).

34. Aleksandr Fursenko and Timothy Naftali, *"One Hell of a Gamble": Khrushchev, Castro, Kennedy and the Cuban Missile Crisis, 1958–1964* (London: John Murray, 1997). See, also, David E. Murphy, Sergei A. Kondrashev, George Bailey, *Battleground Berlin* (New Haven: Yale University Press, 1999); and Richard Breitman, Norman J. W. Goda, Timothy Naftali, and Robert Wolfe, *U.S. Intelligence and the Nazis* (Cambridge: Cambridge University Press, 2005).

35. Jeffrey T. Richelson, *A Century of Spies* (New York: Oxford University Press, 1995).

36. David F. Rudgers, *Creating the Secret State: The Origins of the Central Intelligence Agency* (Lawrence: University Press of Kansas, 2000).

37. Bradley F. Smith, *The Shadow Warriors: OSS and the Origins of the CIA* (London: André Deutsch, 1981).

38. Thomas F. Troy, *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1981).

39. Michael Warner, ed., *The CIA Under Harry Truman, CIA Cold War Records* (Washington, DC: History Staff, Center for the Study of Intelligence, Central Intelligence Agency, 1994). See, also, Arthur B. Darling, *The Central Intelligence Agency* (Washington, DC: History Staff, CIA, 1989).

40. Robin Winks, *Cloak and Gown: Scholars in the Secret War* (New York: William Morrow, 1987).

41. Amy B. Zegart, *Flawed by Design: the Evolution of the CIA, JCS, and NSC* (Stanford: Stanford University Press, 1999).

42. David A. Charters, "British Intelligence in the Palestine Campaign," *Intelligence and National Security* 6 (January 1991), pp. 229–39; John Ferris, "Intelligence," in

R. Boyce and J. Maiolo, eds., *The Origins of World War Two: The Debate Continues* (Basingstoke: Palgrave, 2003).

43. A. Stuart Farson, David Stafford, and Wesley K. Wark, eds., *Security and Intelligence in a Changing World: Perspectives for the 1990s* (London: Cass, 1991). See, also: Wesley K. Wark, ed., *Espionage: Past, Present, Future?* (London: Frank Cass, 1994).

44. Wolfgang Krieger, "German Intelligence History: A Field in Search of Scholars," *Intelligence and National Security* 19 (Summer 2004), pp. 185–98.

45. Karalekas, *History of the Central Intelligence Agency,* op. cit.; and Phyllis Provost McNeil, "The Evolution of the U.S. Intelligence Community—An Historical Perspective," in *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, Report of the Commission on the Roles and Capabilities of the United States Intelligence Community (the Aspin-Brown Commission, led by former Secretaries of Defense Les Aspin and, subsequently, Harold Brown), March 1, 1996, Appendix A.

46. Loch K. Johnson, *Season of Inquiry,* op. cit.; Smist, op. cit.

47. Mark M. Lowenthal, *U.S. Intelligence: Evolution and Anatomy*, 2nd ed. (Westport, CT: Praeger, 1992); Jeffrey T. Richelson, *The U.S. Intelligence Community*, 4th ed. (Boulder: Westview Press, 1999). See, also, Loch K. Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (New Haven: Yale University Press, 1996).

48. Ray S. Cline, *The CIA Under Reagan, Bush, and Casey: The Evolution of the Agency from Roosevelt to Reagan* (Washington, DC: Acropolis, 1981).

49. Glenn Hastedt, "Organizational Foundations of Intelligence Failure," in *Intelligence Policy and Process*, edited by Alfred C. Maurer, Marion D. Tunstall, and James M. Klagle (Boulder: Westview Press, 1985), pp. 140–56; Amy B. Zegart, "September 11 and the Adaptation Failure of U.S. Intelligence Agencies," *International Security* 29 (Spring 2005), pp. 78–111.

50. Christopher Andrew, *Secret Service: The Making of the British Intelligence Community* (London: Sceptre, 1991); Andrew and Gordievsky, op. cit.

51. Jeffrey T. Richelson and Desmond Ball, *The Ties That Bind: Intelligence Cooperation Between the UK/USA Countries* (Boston: Allen and Unwin, 1985). See, also: David Staffaord and Rhodri Jeffreys-Jones, eds., "American-British-Canadian Intelligence Relations, 1939–2000," special issue of *Intelligence and National Security* 15 (2000); and Bradford Westerfield, "America and the World of Intelligence Liaison," *Intelligence and National Security* 11 (1996), pp. 523–60.

52. For example, Richard K. Betts, "Warning Dilemmas: Normal Theory vs. Exceptional Theory," *Orbis* 26 (Winter 1983), pp. 829–33.

53. Philip H. J. Davies, "Ideas of Intelligence: Divergent National Concepts and Institutions," *Harvard International Review* (Autumn 2002), pp. 62–66.

54. Michael I. Handel, "The Study of Intelligence," *Orbis* 26 (Winter 1983), pp. 817–21.

55. Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996); this important book is an example of solid research that could fit into many categories in this chapter (history, for instance), but it is placed under theory because it provides a seminal blending of intelligence history and the author's understanding of public administration—all tempered by the hands-on experience of a former insider in British intelligence.

56. Arthur S. Hulnick, "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach," *Intelligence and National Security* 1 (May 1986), pp. 212–33.

57. Loch K. Johnson, "Bricks and Mortar for a Theory of Intelligence," *Comparative Strategy* 22 (Spring 2003), pp. 1–28, and *America's Secret Power: The CIA in a Democratic Society* (New York: Oxford University Press, 1989).

58. Rob Johnson, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, CIA, 2005).

59. David Kahn, "An Historical Theory of Intelligence," *Intelligence and National Security* 16 (2001), pp. 79–92.

60. Walter Laqueur, *A World of Secrets: The Uses and Limits of Intelligence* (New York: Basic, 1985).

61. Kenneth G. Robertson, ed., *British and American Approaches to Intelligence* (Basingstoke: Macmillan, 1987).

62. Abram Shulsky, *Silent Warfare—Understanding the World of Intelligence* (London: Brassey's, 1993).

63. *Intelligence and National Security* 19 (Summer 2004); see especially in this volume: Len Scott and Peter Jackson, "The Study of Intelligence in Theory and Practice," pp. 39–169; and Christopher Andrew, "Intelligence, International Relations and 'Under-theorization,' " pp. 170–84.

64. Kristin M. Lord and Bernard I. Finel, "The Surprising Logic of Transparency," *International Studies Quarterly* 43 (1999), pp. 315–39.

65. For an example of an innovative study linking intelligence to other aspects of international affairs, see John Stempel, "The Impact of Religion on Intelligence," *International Journal of Intelligence and CounterIntelligence* 18 (2005), pp. 280–95.

66. Matthew Aid and Cees Wiebes, eds., *Secrets of Signals Intelligence During the Cold War and Beyond, Special Issue of Intelligence and National Security* 16 (2001); James Bamford, *The Puzzle Palace* (Boston: Houghton Mifflin, 1984); David Kahn, *The Codebreakers* (New York: Macmillan, 1967); Patrick R. Keefe, *Chatter* (New York: Random House, 2005).

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

68. Jeffrey T. Richelson, *The Wizards of Langley* (Boulder: Westview Press, 2002).

69. Frederick P. Hitz, *The Great Game: The Myth and Reality of Espionage* (New York: Knopf, 2004).

70. Reuel Marc Gerecht, "A New Clandestine Service: The Case for Creative Destruction," in Peter Berkowitz, ed., *Future of American Intelligence* (Palo Alto, California: Hoover Institution Press, 2005), 103–38.

71. See, for example, Robert David Steele, "Relevant Information and All-Source Analysis: The Emerging Revolution," *American Intelligence Journal* 19 (1999), pp. 23–30.

72. Robert Jervis, "Intelligence and Foreign Policy," *International Security* 2 (1986–87), pp. 141–61.

73. Richard K. Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 3 (1978), pp. 961–88.

74. Jack Davis, "A Policymaker's Perspective on Intelligence Analysis," *Studies in Intelligence* 38 (1995), pp. 7–15.

75. Klaus Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," *World Politics* 16 (April 1984), pp. 456–75.

76. Ehraim Kahana, "Early Warning Versus Concept: The Case of the Yom Kippur War, 1973," *Intelligence and National Security* 17 (Summer 2002), pp. 81–104.

77. John Prados, *The Soviet Estimate: U.S. Intelligence Analysis and Russian Military Strength* (New York: Dial, 1982); see, also, Donald P. Steury, ed., *Intentions and Capabilities: Estimates on Soviet Strategic Forces, 1950–1983* (Washington, DC: CIA, 1996).

78. Richard L. Russell, "CIA's Strategic Intelligence in Iraq," *Political Science Quarterly* 117 (Summer 2002), pp. 191–207.

79. Loch K. Johnson, *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security* (New York: New York University Press, 2000).

80. Mark M. Lowenthal, "Tribal Tongues: Intelligence Consumers, Intelligence Producers," *Washington Quarterly* 15 (Winter 1992), pp. 157–68.

81. Harry Howe Ransom, "The Politicization of Intelligence," in a valuable anthology edited by Stephen J. Cimbala, *Intelligence and Intelligence Policy in a Democratic Society* (Dobbs Ferry, NY: Transnational, 1987), pp. 25–46.

82. James J. Wirtz, "Intelligence to Please? The Order of Battle Controversy During the Vietnam War," *Political Science Quarterly* 106 (Summer 1991), pp. 239–63.

83. See, for example, Stewart A. Baker, "Should Spies Be Cops?" *Foreign Policy* 97 (1994–95), pp. 36–52.

84. Glenn Hastedt, "Public Intelligence: Leaks as Policy Instruments—The Case of the Iraq War," *Intelligence and National Security* 20 (September 2005), pp. 419–39.

85. David Wise, *Nightmover* (New York: Random House, 1992). See, also, David Wise, *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America* (New York: Random House, 2002); John Barron, *Breaking the Ring* (Boston: Houghton Mifflin, 1987); and David C. Martin, *Wilderness of Mirrors* (New York: Harper and Row, 1980).

86. Tom Mangold, *Cold Warrior* (New York: Simon & Schuster, 1991).

87. Stan A. Taylor and Daniel Snow, "Cold War Spies: Why They Spied and How They Got Caught," *Intelligence and National Security* 12 (April 1997), pp. 101–25.

88. Hayden B. Peake, "OSS and the Venona Decrypts," *Intelligence and National Security* 12 (July 1997), pp. 14–34.

89. Katherine A. S. Sibley, *Red Spies in America: Stolen Secrets and the Dawn of the Cold War* (Lawrence: University Press of Kansas, 2004).

90. Nigel West, ed., *The Faber Book of Espionage* (London: Faber & Faber, 1993).

91. David Cole and James X. Dempsey, *Terrorism and the Constitution* (New York: New Press, 2006); Daniel S. Gressang IV, "Audience and Message: Assessing Terrorist WMD Potential," *Terrorism and Political Violence* 13 (2001), pp. 83–106; Katherina von Knop, Heinrich Neisser, and Martin van Creveld (Hrsg.), *Countering Modern Terrorism: History, Current Issues and Future Threats* (Bielefeld, Germany: W. Bertelsmann Verlag, 2005); Richard H. Shultz, Jr. and Andrea J. Dew, *Insurgents, Terrorists, and Militias: The Warriors of Contemporary Combat* (New York: Columbia University Press, 2006).

92. Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden* (New York: Penguin, 2004).

93. William J. Daugherty, *Executive Secrets: Covert Action and the Presidency* (Lexington: University Press of Kentucky, 2004).

94. Roy Godson, ed., *Intelligence Requirements for the 1980s: Covert Action* (Washington, DC: Transaction Books, 1981).

95. Richard H. Immerman, *The CIA in Guatemala: The Foreign Policy of Intervention* (Austin: University of Texas Press, 1982).

96. Loch K. Johnson, "Covert Action and Accountability: Decision-Making for America's Secret Foreign Policy," *International Studies Quarterly* 33 (March 1989), pp. 81–109. See, also, Johnson, *Secret Agencies,* op. cit.

97. Stephen F. Knott, *Secret and Sanctioned: Covert Operations and the American Presidency* (New York: Oxford University Press, 1996).

98. Kevin A. O'Brien, "Interfering With Civil Society: CIA and KGB Covert Political Action During the Cold War," *International Journal of Intelligence and CounterIntelligence* 8 (Winter 1995), pp. 431–56.

99. John Prados, *Presidents' Secret Wars: CIA and Pentagon Covert Operations From World War II Through Iranscam* (New York: Quill, 1985), and *Lost Crusader: The Secret Wars of CIA Director William Colby* (New York: Oxford University Press, 2002).

100. W. Michael Reisman and James E. Baker, *Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law* (New Haven: Yale University Press, 1992).

101. Gregory F. Treverton*, Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, 1987).

102. Stephen R. Weissman, "CIA Covert Action in Zaire and Angola: Patterns and Consequences," *Political Science Quarterly* 94 (Summer 1979), pp. 263–86.

103. Peter Wyden, *Bay of Pigs: The Untold Story* (New York: Simon & Schuster, 1979).

104. See "Covert Action," *Hearings*, Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee), Washington, DC (October 23, 1975); Church Committee, "Alleged Assassination Plots," op. cit.; and Church Committee, Final Report, op. cit. On the question of assassination, see also: Jeffrey Richelson, "When Kindness Fails: Assassination as a National Security Option," *International Journal of Intelligence and CounterIntelligence* 15 (2002), pp. 243–74. For Senator Church's views on covert action, see his "Covert Action: Swampland of American Foreign Policy," *Bulletin of the Atomic Scientists* 32 (February 1976), pp. 7–11.

105. Kermit Roosevelt, *Countercoup: The Struggle for the Control of Iran* (New York: McGraw-Hill, 1981); David Wise and Thomas B. Ross, *The Invisible Government* (New York: Random House, 1964).

106. Robert Baer, *See No Evil* (New York: Crown, 2003); Harry Rositzke, *The CIA's Secret Operations: Espionage, Counterespionage, and Covert Action* (New York: Reader's Digest Press, 1977); Michael Scheuer, *Imperial Hubris* (Washington, DC: Brassey's, 2004); and Theodore G. Shackley, *The Third Option: An American View of Counter-insurgency Operations* (New York: Reader's Digest Press). See, also, Duane R. "Dewey" Clarridge, with Digby Diehl, *A Spy for All Seasons: My Life in the CIA* (New York: Scribner's, 1997); and Gary Berstsen, *Jawbreakers* (New York: Crown, 2006).

107. Bob Woodward, *VEIL: The Secret Wars of the CIA, 1981–1987* (New York: Simon & Schuster, 1987). See, as well, James Risen, *State of War: The Secret History of the C.I.A. and the Bush Administration* (New York: Free Press, 2006).

108. William S. Cohen and George J. Mitchell, *Men of Zeal: A Candid Inside Story of the Iran-Contra Hearings* (New York: Viking, 1988). For the official government report on the Iran-*contra* affair, see Senate Select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition and House Select Committee to Investigate

Covert Arms Transactions with Iran, *Hearings and Final Report* (Washington, DC: Government Printing Office, 1987).

109. Jennifer D. Kibbe, "The Rise of the Shadow Warriors," *Foreign Affairs* 83 (2004), pp. 102–15.

110. David M. Barrett, *The CIA and Congress: The Untold Story from Truman to Kennedy* (Lawrence: University Press of Kansas, 2005).

111. Frederick P. Hitz, "Unleashing the Rogue Elephant: September 11 and Letting the CIA Be the CIA," *Harvard Journal of Law & Public Policy* 25 (2002), pp. 756–81.

112. See, for example, Loch K. Johnson, "Congressional Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee," *Public Administration Review* 64 (January/February 2004), pp. 3–14.

113. Frederick M. Kaiser, "Congressional Rules and Conflict Resolution: Access to Information in the House Select Committee on Intelligence," *Congress and the Presidency* 15 (Spring 1988), pp. 49–73, and "Impact and Implications of the Iran-Contra Affair on Congressional Oversight of Covert Action," *International Journal of Intelligence and CounterIntelligence* 7 (1994), pp. 205–34.

114. Harold Hongju Koh, "Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the Iran-Contra Affair," *Yale Law Journal* 97 (June 1988), pp. 1255–1342.

115. Kathryn Olmsted, *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI* (Chapel Hill: University of North Carolina Press, 1996).

116. John M. Oseth, *Regulating United States Intelligence Operations: A Study in Definition of the National Interest* (Lexington: University Press of Kentucky, 1985).

117. Gregory F. Treverton, "Intelligence: Welcome to the American Government," in Thomas E. Mann, ed., *A Question of Balance: The President, the Congress, and Foreign Policy* (Washington, DC: The Brookings Institute, 1990), pp. 70–108.

118. Henry Steele Commager, "Intelligence: The Constitution Betrayed," *New York Review of Books* (September 30, 1976), pp. 32–37.

119. Frank J. Donner, *The Age of Surveillance: The Aims and Methods of America's Political Intelligence Surveillance* (New York: Vintage, 1981).

120. John T. Elliff, *The Reform of FBI Intelligence Operations* (Princeton: Princeton University Press, 1979).

121. Richard E. Morgan, *Domestic Intelligence: Monitoring Dissent in America* (Austin:University of Texas Press, 1980).

122. Frederick A. O. Schwarz Jr. [chief counsel for the Church Committee], "Intelligence Activities and the Rights of Americans," New York Bar Association meeting, New York City (November 16, 1976), reprinted in *Congressional Record* (January 28, 1977), pp. 51627–29.

123. Athan G. Theoharis, *Spying on Americans: Political Surveillance From Hoover to the Huston Plan* (Philadelphia: Temple University Press, 1978).

124. David Wise, *The American Police State: The Government Against the People* (New York: Random House, 1976).

125. Frederic F. Manget, "Another System of Oversight: Intelligence and the Rise of Judicial Intervention," *Studies in Intelligence* 39 (1966), pp. 43–50.

126. For example: Peter Gill, "Reasserting Control: Recent Changes in the Oversight of the UK Intelligence Community," *Intelligence and National Security* 11 (April

1996), pp. 113–331; Mark Phythian, "Still a Matter of Trust: Post-9/11 British Intelligence and Political Culture," *International Journal of Intelligence and CounterIntelligence* 18 (2005–06), pp. 653–81.

127. Reginald Whitaker, *The End of Privacy: How Total Surveillance Is Becoming a Reality* (New York: New Press, 1999).

128. Born, Johnson, and Leigh, op. cit.

129. See, for example, Loch K. Johnson, "Accountability and America's Secret Foreign Policy," *Foreign Policy Analysis* 1 (Spring 2005), pp. 99–120, and "Supervising the Secret Foreign Policy: A Shock Theory of Congressional Oversight for Intelligence," in David P. Forsythe, Patrice C. McMahon, and Andrew Wedeman, eds., *American Foreign Policy in a Globalized World* (New York: Routledge, 2006), pp. 259–77.

130. James A. Barry, "Covert Action Can Be Just," *Orbis* 37 (Summer 1993), pp. 375–90; E. Drexel Godfrey Jr., "Ethics and Intelligence," *Foreign Affairs* 56 (April 1978), pp. 624–42; Michael Herman, "Modern Intelligence Services: Have They a Place in Ethical Foreign Policies?" in Shukman, op. cit. On the ethical issue of protecting U.S. sources abroad, see Frank Snepp, *Decent Interval* (London: Allen Lane, 1980).

131. Among the most prominent of these commission and committee studies in the United States were the reports produced by the Aspin-Brown Commission, op. cit.; by the Kean Commission (led by former New Jersey governor Thomas Kean), *The 9/11 Commission Report*, the National Commission on Terrorist Attacks Upon the United States (New York: Norton, 2004); and by the Silberman-Robb Commission (led by Judge Laurence H. Silberman and former Senator Charles S. Robb), *Final Report*, Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Washington, DC, 2004). With respect to the controversy over faulty intelligence judgments about WMDs in Iraq, the British government produced two influential reports: Lord Butler's *Review of Intelligence on Weapons of Mass Destruction* (London, 2004) and Lord Hutton's *Report of the Inquiry Into the Circumstances Surrounding the Death of Dr. David Kelly* (London, 2004). See, also: Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, *Final Report*, U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, the Graham-Goss Committees, led by Senator Bob Graham, D, Florida, and Representative Porter J. Goss, R, Florida (Washington, DC: December 2002); and *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*, Select Committee on Intelligence, U.S. Senate (Washington, DC: 2004).

132. John H. Hedley, "The Intelligence Community: Is It Broken? How to Fix It," *Studies in Intelligence* 39 (1996), pp. 11–19; Arthur S. Hulnick, *Fixing the Spy Machine* (Westport, CT: Praeger, 1999), and *Keeping Us Safe: Secret Intelligence and Homeland Security* (Westport, CT: Praeger, 2004); Allan E. Goodman, Gregory F. Treverton, and Philip Zelikow, *In From the Cold* (New York: Twentieth Century Fund, 1996); Loch K. Johnson, "The Failures of U.S. Intelligence and What Can Be Done About Them," *Yale Journal of International Affairs* 2 (February 2006); Lt. Gen. William E. Odum, *Fixing Intelligence* (New Haven: Yale University Press, 2002); Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005); and Michael A. Turner, *Why Secret Intelligence Fails* (Washington, DC: Potomac, 2004).

133. See, for instance, Stafford T. Thomas, "The CIA's Bureaucratic Dimensions," *International Journal of Intelligence and CounterIntelligence* 12 (Winter 1999), pp. 399–413.

134. See William E. Colby and Peter Forbath, *Honorable Men: My Life in the CIA* (New York: Simon & Schuster, 1978); Allen Dulles, *The Craft of Intelligence* (Westport, CT: Greenwood, 1977); Robert M. Gates, *From the Shadows* (New York: Simon & Schuster, 1996); Richard Helms, with William Hood, *A Look Over My Shoulder: My Life in the Central Intelligence Agency* (New York: Random House, 2003); and Admiral Stansfield Turner, *Burn Before Reading: Presidents, CIA Directors, and Secret Intelligence* (New York: Hyperion, 2005). See also: John L. Helgerson, *Getting to Know the President: CIA Briefings of the Candidates, 1952–1992* (Washington, DC: CIA Center for the Study of Intelligence, 1996); and Douglas F. Garthoff, *Directors of Central Intelligence as Leaders of the U.S. Intelligence Community, 1946–2005* (Washington, DC: CIA Center for the Study of Intelligence, 2005). On British intelligence, see the elegantly written memoir of a former chair of the Joint Intelligence Committee, Cradock, op. cit.; and on Soviet intelligence, Oleg Kalugin with Fen Montaigne, *The First Directorate: My 32 Years in Intelligence and Espionage Against the West* (London: Smith Gryphon, 1994). The best biographies of American intelligence chiefs are: Peter Grose, *Gentleman Spy: The Life of Allen Dulles* (Boston: Houghton Mifflin, 1994); and Thomas Powers, *The Man Who Kept the Secrets: Richard Helms and the CIA* (New York: Washington Square Press, 1981). For revealing interviews with intelligence managers and operatives, see Ralph Edward Weber, *Spymasters: Ten CIA Officers in Their Own Words* (Wilmington: SR Books, 1999); and for one legendary CIA operative's recollections, Ted Shackley with Richard A. Finney, *Spymaster: My Life in the CIA* (Dulles: Potomac Books, 2005). See, also, A. Denis Clift, *Clift Notes: Intelligence and the Nation's Security* (Washington, DC: Joint Military Intelligence College, 2000); and Evan Thomas, *The Very Best Men: Four Who Dared: The Early Years of the CIA* (New York: Simon & Schuster, 1995).

135. See, for example, Admiral Stansfield Turner, *Secrecy and Democracy: The CIA in Transition* (Boston: Houghton Mifflin, 1985).

136. One example: Daniel Patrick Moynihan, *Secrecy: The American Experience* (New Haven: Yale University Press, 1998).

2

CLOAKS, DAGGERS, AND IVORY TOWERS

Why Academics Don't Study U.S. Intelligence

AMY B. ZEGART

U.S. INTELLIGENCE AGENCIES HAVE NEVER BEEN MORE important and less understood. During the Cold War, the Soviet Union had territory on a map, officials in embassies, and a military that wore uniforms and paraded missiles through Red Square. Today, the principal threat to U.S. national security no longer comes from great powers with return addresses and massive military might, but from small bands of transnational terrorists driven by fanaticism, hidden from view, and armed with deadly weapons that can be concealed in a suitcase or vial. In the Cold War, when the enemy was easy to detect, the first and last line of defense was military power. Now it is intelligence.

Yet since September 11, 2001, many have questioned the basic competence of America's intelligence agencies. The congressional intelligence committees,[1] the 9/11 Commission,[2] the Silberman-Robb Commission,[3] and a seemingly endless parade of press reports all have exposed grave shortcomings and raised troubling doubts about the effectiveness of the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the fourteen other agencies of the U.S. intelligence community. Such fault finding is not new. As early as 1948, the *New York Times* castigated a newly created CIA as "one of the weakest links in our national security,"[4] and since then, forty reports have investigated and examined the performance of U.S. intelligence agencies. But the stakes have rarely been higher and the deficiencies rarely so fundamental. Why did the CIA and FBI fail to capitalize on numerous opportunities to disrupt the 9/11 plot?[5] Why did the intelligence community produce such flawed assessments about Iraq's weapons of mass destruction capabilities? And why, despite the worst terrorist attacks in U.S. history and a massive legislative overhaul, is the intelligence community still unable to operate as a coherent whole?[6] The twin intelligence

failures of 9/11 and the Iraq War have led many to ask whether an intelligence apparatus built for a different enemy at a different time can adapt, and if so, how.

Academics have been strikingly absent from the debate. This chapter explores why. I begin by presenting the evidence of absence, showing how little attention professors at leading U.S. research universities pay to teaching and research about intelligence. Next, I examine the barriers in both academia and the political realm that prevent career academics from studying intelligence issues. Finally, I examine the consequences of neglect for the public's understanding of intelligence and for prospects of intelligence reform.

MISSING INTELLIGENCE ON CAMPUS

Major research universities devote surprisingly little attention to the study of U.S. intelligence issues. In 2006, just four of the top twenty-five U.S. universities ranked by *U.S. News & World Report*[7] offered undergraduate courses on the U.S. intelligence community.[8] In fact, undergraduates at America's elite universities had greater opportunities to learn about the rock band U2 than the spy plane by the same name; more of the top 25 U.S. universities offered courses on the history of rock and roll than on U.S. intelligence.[9]

Scholarly inattention is even more glaring in academic publishing. Between 2001 and 2006, the three most highly regarded academic journals in political science—the *American Political Science Review*, the *American Journal of Political Science*, and *Journal of Politics*[10]—published a total of 750 articles. Only one, an article examining public opinion about trade-offs between civil liberties and security after September 11[11], discussed intelligence.[12]

International relations journals—which are considered less prestigious but are more targeted to an audience of international relations scholars and practitioners—are not much better. Since 2001, the top four international relations field journals—*International Organization*, *World Politics*, *International Studies Quarterly*, and *International Security*—have published nearly 500 articles.[13] Only five have covered intelligence topics. These figures suggest an astounding disconnect between policy makers and academics. At precisely the time that intelligence issues have dominated headlines and policy-maker attention, 99.5 percent of the best articles produced by political scientists have been discussing research about other topics.

Finally, although the September 11 terrorist attacks have spawned a book-publishing frenzy about intelligence problems and the war on terrorism, nearly all of these post-9/11 books have been penned by policy makers and journalists, not by academics. Well-known public officials-cum-authors include former White House counterterrorism czar Richard Clarke,[14] former Senate Intelligence Committee Chairman Bob Graham,[15] former FBI Director Louis Freeh,[16] former CIA bin Laden Unit chief Michael Scheurer,[17] and Circuit Court Judge Richard

A. Posner.[18] Journalists have been equally prolific. Among the legions of current and former reporters, producers, freelance writers, and editors who have published books about the U.S. intelligence community since 9/11 are James Risen from the *New York Times*,[19] Steve Coll and Bob Woodward from the *Washington Post*,[20] Bill Gertz of the *Washington Times*,[21] Terry McDermott of the *Los Angeles Times*,[22] and ABC News reporter John Miller.[23] Only a handful of career academics have joined the fray.[24] Nearly everyone, it seems, has something to say about U.S. intelligence after 9/11 except professors.

TWO BARRIERS TO THE STUDY OF INTELLIGENCE

Why is this the case? Two types of barriers are to blame. The first lies inside the ivory tower and involves the professional norms and incentives that drive career academics to research certain topics and not others. The second exists in the real world and involves the impediments to wresting facts from secret agencies.

The Perils of Theory

At first glance, political science appears to be a natural home for conducting research about the U.S. intelligence community. The problem is that political science is driven by theoretical, not policy questions, and U.S. intelligence agencies lie in a theoretical no-man's-land; they are caught between the political science fields of international relations and American politics.

For international relations scholars, the most interesting theoretical terrain covers relations between states, not what goes on inside them. Do states balance against great powers or bandwagon with them? Do they seek absolute increases in power, prosperity, and other benefits or care more about their relative position in the international pecking order? Did the Cold War peace stem more from the bipolar structure of the international system or the advent of nuclear weapons? These are some of the classic questions in international relations theory. Although some have studied inside-the-state variables and issues,[25] even the most popular recent arguments in international relations—such as Joseph Nye's work on "soft power" and Samuel Huntington's "Clash of Civilizations"—still gaze beyond national borders, at how American values or conflicts between civilizations shape international dynamics, rather than looking within them, at how a country's intelligence agencies operate.[26]

On the other hand, American politics scholars do look at the bureaucracy, but they focus almost exclusively on domestic policy agencies, and regulatory agencies in particular. Here too, theoretical agendas explain why. The central concern driving most research in American politics is the delegation of political power—understanding when and why elected officials voluntarily give some of

their own authority to unelected government bureaucrats. The answers have varied, but all of them place great weight on the role of organized interests and the electoral incentives of legislators. This theoretical focus has naturally led scholars to examine domestic regulatory agencies like the Federal Trade Commission, Interstate Commerce Commission, and the Environmental Protection Agency, where interest groups are strong and where legislators have powerful reasons to care about what those groups want. In the 1970s and 1980s, the rage was capture theory, which argued that private industry designed and operated government agencies for its own benefit.[27] More recently, political scientists have used transaction cost economics to argue that Congress designs and oversees the bureaucracy in surprisingly efficient ways. This work, called the new institutionalism, has taken new ideas but continued applying them to the same old agencies.[28] In the quest to build theory, scholars have paid inordinate attention to domestic regulatory agencies and ignored the rest of the bureaucratic universe.

These abstract debates have real consequences, creating powerful social norms about what constitutes "important work" and career incentives that direct scholarly attention in some directions and away from others. The process starts early, in graduate school. In top political science Ph.D. programs, doctoral students are taught the canon of important theoretical work in class, are often expected to critique theoretical debates in comprehensive field exams before beginning their dissertations, and are ultimately judged by how much and how well their dissertation research contributes original insights to existing academic debates. Degrees are awarded, jobs are gotten, grants are won, tenure is secured, and reputations are made more often by producing the most theoretically interesting research, not by examining the most important government agencies or pressing political issues.

The Perils of Secrecy

Features unique to academia make the benefits of studying U.S. intelligence low. At the same time, features unique to intelligence make the costs of studying intelligence exceptionally high.

No organization is easily studied from the outside. In private firms, nonprofit organizations, and government agencies, the formal mission and structure often reveal little about the "real" inner workings of the organization. Intelligence agencies, however, are particularly difficult for outsiders to study, for two reasons.

The first and most obvious reason is classification—or, more precisely, the over-classification of information. The current classification system arose during the Cold War, when government officials kept paper records, managed information by hand instead of computers, and erred on the side of classifying more rather than less. By the 1990s, this system had become unmanageable. In 1997, the Commission on Protecting and Reducing Government Secrecy, chaired by the late Senator Daniel Patrick Moynihan, found that roughly three million people in government and industry had the ability to classify information, and all of them

were operating without consistent guidelines or statutory standards. "Apart from aspects of nuclear energy subject to the Atomic Energy Act," the commission concluded, "secrets in the Federal Government are whatever anyone with a stamp decides to stamp secret."[29]

The result has been an intelligence system where much remains inaccessible to the outside. Those interested in studying environmental policy, for example, can access more than thirty years of detailed budgetary data from the Environmental Protection Agency. By contrast, the grand total of the U.S. intelligence community's budget has been publicly released only twice, in fiscal years 1997 and 1998, producing a cottage industry of outsiders who scour news stories, congressional documents, and commission reports for clues to make intelligence spending estimates.

The Freedom of Information Act (FOIA), first passed in 1966, allows any person to request the release of classified documents, and by law federal agencies must respond to all requests within 30 business days.[30] In reality, however, the FOIA process is time-consuming, cumbersome, and riddled with uncertainty. For starters, "response" means providing a status report of the request, not resolving it. More often, the actual processing period to determine whether a document will be released lasts months, even years. Since 1996, all federal agencies have been required to report statistics about their handling of FOIA requests. According to the CIA's records, the agency's fastest year was 2005, when the median time it took to resolve the backlog of pending FOIA requests was 324 business days, or fifteen calendar months.[31] The worst recorded year was 2001, when the median response time was 605 days, or nearly two and half years.[32] And of course, the median means that half of these requests took longer than 605 days to resolve—in some cases, much longer. According to a 2003 audit by the National Security Archive at George Washington University, the oldest pending FOIA requests were filed during the Cold War. In one, for example, a University of Southern California graduate student, William Aceves, requested Defense Department records on the U.S. "Freedom of Navigation" program. He sent the request in 1989. When the National Security Archive conducted its audit fourteen years later, Aceves had become a full professor, was still interested in the records for his research, and was still waiting to hear whether he would ever receive them.[33]

His is by no means an isolated case. The National Security Archive audit found that in 2003, the FBI's ten oldest pending FOIA requests were between three and sixteen years old. The Defense Intelligence Agency's ten oldest requests had originally been filed seven to twelve years earlier. And the CIA's ten oldest requests had all been pending for more than fourteen years.[34]

It may be that academic researchers can obtain classified information about a host of subjects more quickly and easily than these figures suggest. The problem, however, is that they can never be sure. There is no way to know ahead of time whether any particular FOIA request will take days, weeks, months, or years to process. The uncertainty inherent in the declassification system, in short, provides strong incentives for academics to steer clear of intelligence. Few career-minded

academics are willing to risk their futures that newly declassified research materials are on the way.

The second reason that career academics have a hard time studying intelligence is closely related to the first: Classification has engendered a culture of secrecy inside the intelligence community that makes even unclassified information difficult for outsiders to obtain. Evidence is the lifeblood of research, and it comes in three forms: data sets, documents, and people. All are exceptionally difficult to find in the U.S. intelligence community.

Consider what at first glance would seem to be the easiest information to gather: the number of congressional hearings about different intelligence issues over time. It turns out that even this information is not so easily found. Intelligence is handled by at least eight major congressional committees, each of which provides whatever information it wants in whatever form it desires on its own website. No one, apparently, has thought to consider what minimum information should be provided consistently—say, an annual, updated list of committee hearing dates, topics, and a designation of whether hearings are open or closed to the public. Although the Congressional Information Service is considered the most reliable index of congressional hearings, it does not always publish hearing transcripts quickly (lag times run up to three years between the date of the hearing and its appearance in the index). The index does not mention whether particular hearings are open or closed to the public, raising questions about the accuracy and comprehensiveness of search results. My point is not that committee hearing information is impossible to find but that it is far more difficult to find than it should be, particularly in a research area where everything else is even more inaccessible.

As one might expect, obtaining executive branch documents is more challenging. This is because intelligence agencies still retain a great deal of discretion over what information they release, to whom, and when. This gatekeeping role, combined with the intelligence community's natural penchant for holding information closely rather than sharing it broadly, has created a universe of information that is unclassified but effectively off limits to outsiders. In November 2004, for example, I called the FBI director's office and requested two sets of documents: an unclassified version of the Bureau's 1998 strategic plan, and historical data about which FBI officials had won presidential rank awards—the government's highest civil service honor—between 1991 and 1998. I was quickly sent to the Bureau's office of public affairs, which advised that a Freedom of Information Act request would probably have to be filed. When I pointed out that the documents were not classified, that the Bureau had in fact referred to presidential rank awards in some of its own public documents,[35] and that the names of all winners from 1998 to 2004 were publicly listed on another federal government website,[36] I was told information would be forthcoming. As of this writing it was October 2006 and I was still waiting.

People, finally, are crucially important for understanding the inner workings of U.S. intelligence agencies. But even locating the right people to interview is

far more challenging in intelligence than in most other policy areas. Scholars interested in interviewing key EPA personnel, for official business, need only search the agency's online personnel directory. At the CIA, the total number of employees is classified, and no online directory exists for officials without undercover responsibilities. Even the CIA's Director of Public Affairs, Mark Mansfield, has no direct contact information posted online.[37]

What's more, Cold War–era intelligence security procedures still strongly discourage contact with outsiders, even when it benefits the intelligence community. In 2004, for example, the CIA's Office of Security called a senior intelligence official and asked why he had been speaking with so many academics and other external contacts. The official explained that communicating with outside experts was part of his official job responsibilities set out by the Director of Central Intelligence. He was brought in for questioning anyway and spent four hours the next day taking a polygraph test. "I didn't care," he later reflected. "But imagine if I were a GS-13. No way would I be talking to anybody again. We keep hiring people and giving them titles like Director of Outreach. But nobody's told the security guys."[38]

In short, classified information is hard to get and unclassified information is not much better: When it comes to the intelligence business, public does not mean accessible. Over fifty years, the community's classification system, cultural affinity for secrecy, and reliance on bureaucratic procedures have produced a thicket through which information does not pass easily.

Enterprising academics certainly can overcome these barriers. But most never try because doing so is costly and more attractive alternative research topics are plentiful. Indeed, gathering information about U.S. intelligence issues and agencies requires the one thing in shortest supply for most academics: time. The well-worn image of tweedy professors lounging in coffeehouses, pouring over old books, and pondering endlessly is nowhere close to the reality now confronting professors in major research universities. A more accurate view is captured by the phrase "publish or perish." Young professors are given between seven and ten years to make their scholarly mark in the world or they are denied tenure and fired, often with little hope of landing another academic job any time soon. Most universities, in fact, operate with tight restrictions about the timing, expertise, and number of faculty appointments, creating a job market that is inefficient and incapable of hiring to meet surging educational needs or snatching good people when they are cast adrift in the tenure process elsewhere. The ticking tenure clock creates strong incentives for rising academics to research topics with data that is readily available so that publications can be produced quickly. Those topics are found more often and more reliably outside the U.S. intelligence community.

In sum, it should come as no surprise that intelligence has not been a hot topic in academia. U.S. intelligence agencies have been largely ignored because they are too domestic for international relations theorists and too foreign for scholars of American politics, because social norms and incentives discourage

most scholars from venturing too far from the main intellectual currents of their fields, because it is exceptionally difficult for academics to get their hands on intelligence information for their work, and because plenty of other topics are easier to study.

WHY ACADEMICS MATTER

Some readers may be wondering, "So what if academics neglect the study of intelligence?" The short answer is that it matters a great deal. Academic teaching and research have the potential to shape public perceptions about how intelligence agencies actually work and influence policy choices about how to make intelligence agencies work better.

Public Perceptions: Fact Versus Fiction

Most Americans' understanding of U.S. intelligence agencies is based more on fiction than fact. Hit television shows like *Alias* and *24*, James Bond movies and spy novels—Le Carré and Tom Clancy come to mind—are wildly popular but not wildly accurate. As Mark M. Lowenthal, former Assistant Director of Central Intelligence for Analysis and Production, joked, "*Alias* is hardly a realistic portrayal of what we do. For one thing, none of us are that good looking, at least consistently, and none of our cases are ever solved in 42 minutes."[39] The CIA's own website acknowledges the misperception problem. Its homepage for high school students begins by noting, "When people think of the CIA, they think of people lurking around in trench coats, sending messages in code, and using cool tools to do their job."[40]

These examples may seem frivolous, but the danger is real. Americans are steeped in misconceptions about what U.S. intelligence agencies actually do, and misplaced expectations about how well they can do it. James Bond always gets his man and Jack Bauer always saves the United States each television season, but real intelligence officers live in a different world. "On a weekly basis, we are always wrong about something," notes Lowenthal. "That's why we have intelligence agencies, because we don't know."[41]

When public perceptions diverge so much from reality, two problems arise. The first is that the public may judge the intelligence community a failure—even when it may be working well—because perfection is an impossible goal to meet. The second problem is exactly the opposite: The public's confidence in the power and effectiveness of U.S intelligence agencies may be so overblown that policy makers cannot garner support for intelligence reforms, even when they are desperately needed. Ultimately, the gap between public perceptions and policy-making imperatives may become impassable, with the public believing that intelligence agencies are omnipotent and should be restrained, and policy makers believing that they are incompetent and must be strengthened. Academic research

and teaching are vital for bridging this gap—providing a realistic and dispassionate view of the capabilities that U.S. intelligence agencies have, the constraints under which they operate, and the challenges that they face.

Individuals Versus Organizations: The Intelligence Reform Debate

Academics also have the potential to shape intelligence policy debates in Washington by analyzing problems in ways that others do not. Most often, intelligence policy discussions are dominated by policy makers and the journalists who cover them. For most officials and reporters, individuals are the heart of the matter: Intelligence successes and failures are all about who's on top, what skills different people bring to their jobs, and who knows whom. Career academics, by contrast, are taught to avoid these kinds of "it depends on the person" arguments. Instead, professors are trained to develop general explanations that can account for outcomes across specific times, places, and individual leaders. For them, the most important determinants of intelligence success and failure are not individuals, but the forces that transcend them.

The difference between these approaches is most usefully seen by examining accounts of 9/11. In the five years since the World Trade Center and Pentagon attacks, the prevailing wisdom propagated by policy makers and journalists has attributed the tragedy to the failures of individuals. Former Clinton National Security Advisor Samuel Berger, former Secretary of State Madeline Albright, and former White House counterterrorism czar Richard Clarke, among others, have faulted President Bush and his administration for giving terrorism short shrift compared to missile defense and other foreign policy issues. Others, including Secretary of State Condoleezza Rice and Vice President Richard Cheney, have charged the Clinton administration with failing to develop an effective counterterrorism strategy and emboldening bin Laden by responding weakly to earlier terrorist attacks. Journalistic accounts, too, have focused on the role of individuals—on the personalities and personal battles behind the scenes that led to disaster.

These accounts are both understandable and misguided. We are left to think that if only a few important people had connected a few obvious dots, tragedy could have been averted. What is missing is a sense of context, of the underlying constraints and forces that made it likely that talented people would make poor decisions.

An organizational analysis, by contrast, finds three such constraints at work before 9/11: (1) cultural pathologies that led intelligence agencies to resist new technologies, ideas, and tasks after the Cold War ended; (2) perverse career incentives that rewarded intelligence officials for all of the wrong things; (3) and structural weaknesses dating back decades that prevented the U.S. intelligence community from working together as a coherent whole. With technology-phobic FBI agents keeping case files in shoeboxes rather than putting them into computers,

with CIA operatives clinging to old systems designed for recruiting Soviet officials at cocktail parties rather than Jihadists in caves, with career incentives that rewarded intelligence officials for staying cloistered in their own agencies rather than sharing information across agency lines, and with a 40-year-old intelligence structure that gave no person the power to knock bureaucratic heads together, the U.S. intelligence community did not have a fighting chance against Al Qaeda.[42] According to this view, U.S. intelligence agencies failed to stop the terrorist attacks not because individuals made mistakes, but because individual mistakes were the inevitable result of the debilitating organizational deficiencies that had afflicted America's intelligence community for years.

I do not mean to suggest that university professors corner the market when it comes to offering penetrating analysis of the past and bright ideas for the future. What I am suggesting is that the day jobs of policy makers and journalists require different tools and time horizons than professors have, and these differences lead them to very different explanations and solutions. For policy makers and journalists, deadlines are tight, individuals matter, and success hinges on specifics—the details of the treaty, the intricacies of policy, the nuances of the story. As a result, policy makers and journalists tend to exaggerate the role of individual leaders in assessing past failures. They rely on anecdotal evidence that can be collected quickly instead of studying a single problem in systematic detail over a number of years. And they tend to favor reforms that address specific failings of the past. Professors, in contrast, are paid to search for general cause-and-effect relationships. They are trained to gather comprehensive evidence to support or refute hypotheses. And they naturally gravitate toward reforms that address the general problems they find. Thus, even when professors, journalists, and government officials examine the same problem, they are likely to focus on separate pieces of the puzzle, offer differing explanations, marshal distinct kinds of evidence, and suggest different implications.

CONCLUSION

American intelligence agencies need help now more now than ever. With the Cold War gone, terrorist enemies emerging, and future enemies still unknown, U.S. intelligence agencies face the worst of all worlds: They are hobbled by the structures and ideas of the past and are ill equipped to deal with an uncertain future.

Sixty years ago, at the dawn of the Cold War, academics played a vital role in developing new organizations and new ideas for U.S. national security. Professors on leave from elite universities became some of the CIA's first analysts.[43] On campus, academic research on game theory provided key insights into the logic and workings of nuclear deterrence. Today, the demand for new thinking is just as great, but the obstacles to providing it are greater. Five years after September 11, professors are not flocking to learn about or work inside the U.S.

intelligence community. The reasons have less to do with political views about the CIA or other intelligence agencies than with the professional incentives that career academics face. Restrained by theory on one side and secrecy on the other, professors are unlikely to be delving into the world of James Bond any time soon.

NOTES

1. Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 107th Cong., 2d sess., December 2002.

2. The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton, 2004).

3. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington, DC: Government Printing Office, March 31, 2005).

4. Hanson W. Baldwin, "Intelligence," *New York Times*, 20 July 1948.

5. Together, the CIA and FBI missed twenty-three opportunities to potentially disrupt the September 11 attacks. See Amy B. Zegart, *Failure and Consequence: Understanding U.S. Intelligence and the Origins of 9/11* (Princeton, NJ: Princeton University Press, 2007).

6. See, for example, Walter Pincus, "Some Lawmakers Doubt DNI Has Taken Intelligence Reigns," *Washington Post*, February 2, 2006, p. A09; Michael Isikoff and Daniel Klaidman, "Look Who's Not Talking—Still," *Newsweek*, April 4, 2005, p. 30; Helen Fessenden, "The Limits of Intelligence Reform," *Foreign Affairs* 84 (November/December 2005), pp. 106–120; *Final Report on 9/11 Commission Recommendations*, 9/11 Public Discourse Project, December 5, 2005, available at http://www.9-11pdp.org/press/2005-12-05_report.pdf

7. "Best National Universities," *U.S. News & World Report*, August 29, 2005, Vol. 139, No. 7, p. 80.

8. The four were Duke, Georgetown, the Massachusetts Institute of Technology, and the University of Virginia. Based on analysis of online university course catalogs conducted March 24–31, 2006.

9. Based on analysis of online university course catalogs conducted March 24–31, 2006.

10. Polling of political scientists reveals substantial consensus about the top three general disciplinary journals. For more, see James C. Garrand and Micheal W. Giles, "Journals in the Discipline: A Report on a New Survey of American Political Scientists," *PS: Political Science and Politics*, April 2003, pp. 293–308.

11. Darren W. Davis and Brian D. Silver, "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America," *American Journal of Political Science* 48 (January 2004), pp. 28–46.

12. Based on analysis of titles and abstracts of journal articles from January 2001 through May 2006.

13. The exact total is 491 articles, based on analysis of issues of *International Organization* from January 2001 through January 2006; *World Politics* from January 2001

through April 2005; *International Studies Quarterly* from January 2001 through March 2006; and *International Security* from January 2001 through December 2005.

14. Richard A. Clarke, *Against All Enemies: Inside America's War on Terror* (New York: Free Press, 2004).

15. Bob Graham, with Jeff Nussbaum, *Intelligence Matters: The CIA, the FBI, Saudi Arabia, and the Failure of America's War on Terror* (New York: Random House, 2004).

16. Louis J. Freeh, *My FBI: Bringing Down the Mafia, Investigating Bill Clinton, and Fighting the War on Terror* (New York: St. Martin's, 2005).

17. Michael Scheuer, *Imperial Hubris: Why the West Is Losing the War on Terror* (Dulles, VA: Brassey's, 2004).

18. Richard A. Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11* (Stanford, CA: Hoover Institution Press, 2005); Richard A. Posner, *Remaking Domestic Intelligence* (Stanford, CA: Hoover Institution Press, 2005). A number of other, less well-known former officials have also produced major books. See, for example, Jennifer Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005); Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (New York: Cambridge University Press, 2003); Arthur S. Hulnick, *Keeping Us Safe: Secret Intelligence and Homeland Security* (Westport, CT: Praeger, 2004); Bruce Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century* (New York: Free Press, 2003).

19. James Risen, *State of War: The Secret History of the CIA and the Bush Administration* (New York: Free Press, 2006).

20. Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001* (New York: Penguin, 2004); Bob Woodward, *Plan of Attack* (New York: Simon & Schuster, 2004); Bob Woodward, *Bush at War* (New York: Simon & Schuster, 2002).

21. Bill Gertz, *Breakdown: How America's Intelligence Failures Led to September 11* (Washington, DC: Regnery, 2002).

22. Terry McDermott, *Perfect Soldiers: The 9/11 Hijackers: Who They Were, Why They Did It* (New York: HarperCollins, 2005).

23. John Miller and Michael Stone, with Chris Mitchell, *The Cell: Inside the 9/11 Plot, and Why the FBI and CIA Failed to Stop It* (New York: Hyperion, 2002).

24. See, in particular, Loch K. Johnson, *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Search for Security* (New York: New York University Press, 2002); Loch K. Johnson and James J. Wirtz, eds., *Strategic Intelligence: Windows Into a Secret World* (Los Angeles: Roxbury Press, 2004); Richard K. Betts and Thomas G. Mahnken, eds., *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I Handel* (London: Frank Cass, 2003).

25. See, for example, Graham Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown, 1971); Morton H. Halperin, *Bureaucratic Politics and Foreign Policy* (Washington, DC: Brookings, 1974); James Fearon, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review* 88 (September 1994), pp. 577–92; Kenneth Schultz, *Democracy and Coercive Diplomacy* (New York: Cambridge University Press, 2001).

26. Joseph S. Nye Jr., *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004); Samuel P. Huntington, *The Clash of Civilizations and the Remaking of the World Order* (New York: Simon & Schuster, 1996).

27. George J. Stigler, "The Theory of Economic Regulation," *Bell Journal of Economics and Management Science* 2 (1971), pp. 3–21; Sam Peltzman, "Toward a More General Theory of Regulation," *Journal of Law and Economics* 19 (1976), pp. 211–40; Gary Becker, "A Theory of Competition Among Pressure Groups for Influence," *Quarterly Journal of Economics* 98 (1983), pp. 371–400.

28. See, for example, Barry Weingast and Mark Moran, "Bureaucratic Discretion or Congressional Control? Regulatory Policymaking by the Federal Trade Commission," *Journal of Political Economy* 91 (October 1983), pp. 775–800; Mathew D. McCubbins, "The Legislative Design of Regulatory Structure," *American Journal of Political Science* 29 (November 1985), pp. 721–48; Lawrence S. Rothenberg, *Regulation, Organizations, and Politics: Motor Freight Policy at the Interstate Commerce Commission* (Ann Arbor: University of Michigan Press, 1994).

29. *Report of the Commission on Protecting and Reducing Government Secrecy* (The Moynihan Commission), 103rd Cong., March 3, 1997 (Washington, DC: Government Printing Office, 1997), p. xxii.

30. Usually, agencies have only twenty working days in which to respond. An additional ten-day extension is available for "unusual circumstances." For a thorough discussion of FOIA, see United States Government Accountability Office, Information Management: Implementation of the Freedom of Information Act, Testimony Before the Subcommittee on Government Management, Finance, and Accountability, U.S. House Committee on Governmental Reform, May 11, 2005, GAO 05-648T.

31. Central Intelligence Agency, Freedom of Information Act Annual Report, Fiscal Year 2005, p. 9, available at http://www.foia.cia.gov/annual_report.asp (accessed March 29, 2006). Calculations assume 250 business days in a calendar year.

32. Central Intelligence Agency, Freedom of Information Act Annual Report, Fiscal Year 2001, p. 8, available at http://www.foia.cia.gov/annual_report.asp (accessed March 29, 2006).

33. The National Security Archive, George Washington University, "Justice Delayed Is Justice Denied: Freedom of Information Act Audit: The Ten Oldest Pending FOIA Requests," November 17, 2003, available at http://www.nsarchive.org (accessed March 30, 2006), pp.1–2.

34. The National Security Archive, George Washington University, "Justice Delayed Is Justice Denied: Freedom of Information Act Audit: The Ten Oldest Pending FOIA Requests," November 17, 2003, available at http://www.nsarchive.org (accessed March 30, 2006), p. 5.

35. See, for example, FBI press releases announcing the appointments of Sheri A. Farrar as Assistant Director of the FBI's Administration Services Division, October 30, 2001, available at http://www.fbi.gov/pressrel/pressrel01/mueller103001.htm (accessed March 28, 2006) and the appointment of Gary M. Bald as head of the FBI's new National Security Branch, August 12, 2005, available at http://www.fbi.gov/pressrel/pressrel05/nsbleadership081205.htm (accessed March 28, 2006).

36. http://www.opm.gov/ses/presrankaward.asp (accessed March 28, 2006).

37. See, for example, http://www.cia.gov/cia/information/mansfield.html (accessed Oct. 1, 2006).

38. Confidential interview by author, May 2004.

39. Remarks, Regional Intelligence Conference, University of Southern California and the Center for the Study of Intelligence, Los Angeles, CA, February 2, 2006.

40. http://www.cia.gov/cia/ciakids/who_we_are/mission.shtml (accessed April 19, 2006).

41. Remarks, Regional Intelligence Conference, University of Southern California and the Center for the Study of Intelligence, Los Angeles, CA, February 2, 2006.

42. Amy B. Zegart, "September 11 and the Adaptation Failure of U.S. Intelligence Agencies," *International Security* Vol. 29 (Spring 2005), pp.78–111.

43. Loch Johnson, "The CIA's Weakest Link," *Washington Monthly* (July/August 2001), pp. 9–14.

3

STUDYING INTELLIGENCE

A British Perspective

TIMOTHY GIBBS

A PROMINENT BRITISH ACADEMIC RECENTLY DESCRIBED HIMSELF and other historians as "The Last Customer" of the British intelligence community.[1] The term is a reference to the fact that the growing band of historians specializing in the British intelligence community are the last people to gain access to the output of the U.K. intelligence agencies, through their eventual declassification and transfer to the Public Record Office. Although they are at the back of the line, and although the time delay involved is the cause of some frustration, historians recognize that the release of any intelligence material whatsoever marks a change in British policy and demonstrates a greater degree of openness in the Secret World than had existed before now. Drawing upon the results of this change, and my own experience as a student of intelligence, this chapter will focus on four themes related to the study of this subject in the United Kingdom and attempt a comparison with the American experience.

First, it will discuss the British intelligence community and the three major civilian organizations in some detail and outline their involvement in some of the major intelligence operations of the 20th century. The second theme is an examination of the issue of access to British sources related to intelligence—a contentious subject and the cause of much debate, both inside the intelligence community and in academia. Certainly, the emphasis upon secrecy has been central to the activities of the intelligence services in the United Kingdom, as elsewhere, but recent welcome moves toward a greater degree of transparency have altered the landscape quite dramatically. Third, this chapter will briefly address the historiography of intelligence in the United Kingdom, and how this has been influenced both by the restrictions of secrecy and by the insatiable appetite for popular accounts of intelligence-related activities. Last, it will consider

the appointment of an official historian for the Security Service and the debate surrounding this new development.

The chapter will be broadly historical, reflecting both my own background and the fact that security restrictions mean that contemporary activities are generally beyond detailed examination. Before I begin, I should express two potential conflicts of interest: First, my doctoral research is made possible by the recent policy of declassification that has revolutionized the study of intelligence in the United Kingdom; second, my Cambridge supervisor, Professor Christopher Andrew, is to be the author of the first official history of MI5, due for publication in 2009.

THE BRITISH INTELLIGENCE COMMUNITY

The development and activities of the three major British civilian intelligence agencies in the United Kingdom and their interaction with policy making via the Joint Intelligence Committee are intriguing subjects but have received relatively little serious academic attention. Moreover, academics frequently fail to take into account the "intelligence dimension" when writing about major political and military events. Given the central position of Britain in the 20th century, not least as a major combatant in the two World Wars, this situation should be redressed by dedicated and informed historical study. Also worthy of careful study is the unique nature of the relationship of the British intelligence community with its partner agencies in Washington, which grew out of the close collaboration of the two Allies during World War II. A last area where British intelligence demands academic attention is in its relations with enemy intelligence services, most notably the Soviet Union. Geographic and historical factors have rendered Britain a major target for the Soviet intelligence services. In this connection, the British intelligence community has been involved in some of the most remarkable spy stories ever recorded, including the notorious "Cambridge Five." This episode will be addressed in some detail as an interesting case study with far-reaching ramifications for the study of British intelligence.

The Secret Intelligence Service (SIS)

"The best recruiting sergeant we ever had," was how one senior intelligence officer described the most famous agent of the British intelligence services, James Bond. The Cambridge-educated Scotsman with a penchant for vodka martinis and deadpan one-liners has come to personify the suave and sophisticated nature of the MI6 officer. Regrettably for Ian Fleming fans and despite the author's intelligence background, the image presented in his books and the subsequent films is somewhat divorced from reality. Bond's organization, the Secret Intelligence Service (SIS, also known as MI6), began life in 1909, as an amateurish outfit

intended to collect information on potential enemies in Europe, particularly the growing threat of imperial Germany.[2] In the interwar period it became increasingly concerned with the threat posed by the Comintern and Soviet-inspired revolutionary activity, and by the 1930s was taking an active interest in the expansionist goals of the Japanese, Italians, and Germans. Regrettably, the evidence on specific activities during this period is hampered by the unavailability of most SIS files, but it is believed that the successes in this period were relatively limited. After the end of hostilities in 1945, the SIS was regarded as having had a "good war," but the plaudits mainly stemmed not from the activities of the organization itself, but more from the reflected glory the Service gained through its control of the code-breaking operations at Bletchley Park. In fact, Bletchley Park was run by the Government Code and Cipher School, not the SIS, but they were responsible for the dissemination of the product of the code breakers.

In its position as a foreign intelligence collection agency, the SIS performs a similar role to the American Central Intelligence Agency (CIA). Like the CIA, it has also been involved in operations that went beyond the collection of intelligence, but in comparison with the furor over CIA "covert" operations in Cuba, Iran, and Guatemala, British activities in this area have received little public attention. Interestingly, it has been demonstrated that the successful CIA Iranian operation in 1953, code-named Operation BOOT, was largely instigated by SIS, who regarded the reformist government of Mossadeq as a threat to British interests. Historically, the documented SIS operations that most closely resemble covert action were the attempts by various SIS-affiliated operatives to destabilize Soviet Russia in the immediate aftermath of the Bolshevik Revolution. The most famous of these agents, Sidney Reilly, organized several ambitious plots against the new regime. Using an innovative strategy, he decided against assassination of senior Bolsheviks because his aim was "not to make martyrs of the leaders but to hold them up to ridicule before the world." In pursuit of this goal, he envisaged a scheme involving forcibly removing the trousers of Lenin and Trotsky, and then parading them through the streets of Moscow.[3] Regrettably for the British agent, these operations were frustrated by the work of the Soviet intelligence and Reilly's career ended with his execution in Moscow in 1925 after a successful sting operation.[4]

The precise role of the SIS in events such as the Suez Crisis, the Falklands, and the Gulf Wars remains unclear, but the organization participated in several impressive intelligence collection operations during the Cold War. Probably the most influential operation was the control by the SIS of the Soviet military intelligence organization Glavnoye Razvedyvatelnoye Upravlenie (GRU) defector-in-place, Oleg Penkovsky, who has been dubbed the "Spy Who Saved the World." Penkovsky had initially approached the CIA, but the American agency encountered some difficulties in running him and brought in MI6 to help in the operation. The British organization then proceeded to exploit his exceptional intelligence in partnership with their American allies. Information provided by

Penkovsky is credited with a major role in the peaceful outcome of the Cuban Missile Crisis, as it was through manuals provided by him that the CIA was able to identify the missile launch sites on Cuba before they became operational, and to monitor the deployment on the island. Penkovsky's biographers Jerrold Schecter and Peter Deriabin maintain that the additional time for deliberation that was permitted by this timely intelligence contributed to the peaceful resolution of the crisis.[5] More recently, the SIS have successfully handled the former Soviet State Security or Komitet Gosudarstvennoy Bezopasnosti (KGB) resident in Britain, Oleg Gordievsky, who was able to keep them informed of the Soviet government's increasingly paranoid behavior in the early years of the Reagan administration. In 1991, they were also responsible for exfiltrating the former KGB archivist Vasili Mitrokhin, another major defector who had been turned away by a U.S. legation in one of the Baltic states.[6]

Unlike in the United States, where the CIA came under heavy public and congressional scrutiny in the 1970s, the SIS has managed to maintain a low profile, with the tacit approval of government, who until the late 1980s would not admit its existence in peacetime. However, in 2004 the organization attracted an unaccustomed level of negative publicity during the controversy over the "dodgy dossiers," which were used to support the government's case for participation in the invasion of Iraq. It became evident from the report into the dossier by former Cabinet Secretary Sir Robin Butler that the intelligence provided by the SIS to the Joint Intelligence Committee and used to justify the claims that Saddam Hussein possessed weapons of mass destruction had been misrepresented to the House of Commons, with the connivance of the then Chairman of the Joint Intelligence Committee, John Scarlett. The SIS role in the affair demonstrated the limitations of their intelligence in Iraq and their overdependence on a small number of unreliable sources.

The Security Service (MI5)

The domestic partner to the SIS is the Security Service, still referred to as MI5 though no longer the responsibility of the military authorities. Originally conceived as a counterespionage organization to protect Britain from the imaginary hordes of German spies[7] supposedly unleashed by the kaiser in the early years of the 20th century, MI5 has had a lower profile role than its foreign counterpart the SIS, though the recent BBC television drama *MI5* has upped the glamour stakes quite considerably.[8] During the two World Wars, MI5 was responsible for countering German (and Italian) spying operations in Britain itself and in the Imperial territories, but between the wars the organization's chief concern was internal subversion, particularly when linked to Soviet Communism. Though de-emphasised during the period when the USSR was allied with the West, this anti-Soviet role continued over the course of the Cold War. In the light of the perceived threat of Soviet espionage, MI5 also acquired greater powers and

responsibilities in relation to vetting potential government employees in the 1950s and since the 1960s the Service has became increasingly preoccupied with counterterrorism issues. The first major terrorist threat came from Irish Republicans and their Loyalist opponents in Ulster, but more recently the concern has been Islamist terrorism. Responsibility for counterterrorism was originally split with the Metropolitan Police's Special Branch, but in the 1990s MI5 successfully argued that they should take the lead on this question, using the skills they had developed during the Cold War.

In recent years, and particularly in relation to the events of September 11, 2001, numerous politicians and policy makers in the United States have cast envious glances at MI5, believing that the specialist structure employed by that organization has advantages over the American model. Most specifically, they recognize that separating the innately different activities of counterterrorism and counterespionage from the portfolio of what is largely a crime-fighting organization, the Federal Bureau of Investigation (FBI), would bring some operational benefits. From a historical point of view, it is evident that FBI Director J. Edgar Hoover's preoccupation with arrest figures and ensuring positive publicity for the Bureau had a profound effect on the manner in which the special agents carried out counterespionage operations. Moreover, in relation to the attacks on September 11, the FBI and CIA have been criticized for failure to coordinate their operations and share information on possible threats, prompting some to suggest a new organization to concentrate on the counterterrorism issue.

Some of MI5's greatest achievements in counterintelligence have come in wartime. In both the First and Second World Wars, the German spy networks in Britain were rapidly identified and dealt with by the Security Service. Admittedly, the German espionage apparatus in the 1914–18 conflict was amateur and poorly coordinated, but nonetheless, the threat was rapidly and efficiently neutralized within days of the outbreak of hostilities. During World War II, the activities of the *Abwehr* were considerably more sophisticated.[9] Nonetheless, MI5 was particularly successful at capturing German agents and then using them to relay false information back to Berlin.

> in the next twelve months [from June 1940] MI5 progressed from a state of almost total ignorance about the *Abwehr*'s capacities and intentions to the position in which the influence it could exert over the *Abwehr*'s activities was so great that, far from constituting a threat to Great Britain, the *Abwehr*'s activities were a serious handicap to Germany for the rest of the war.[10]

As well as controlling the enemy's spying activities, British counterintelligence also engaged in extensive strategic deception, relaying false intelligence reports to the Germans. The contribution of the "double cross system" was a major factor in the success of the Normandy landings. Despite this strong performance against German spies, MI5's wartime record against Soviet espionage

was far less impressive, though the true dimensions of this problem were not to manifest themselves until six years after the end of the conflict.

Outside of wartime, it is generally difficult to gauge with a great degree of accuracy the success rate of MI5 operations. In common with other counterintelligence and counterterrorism organizations, the Service is generally unable to publicize its activities because of the concern that this might jeopardize operations. Particularly in counterterrorism failures become public knowledge, whereas the successes normally go undetected by the general public. In relation to counterespionage there have been some notable successes, for example against Soviet illegal Gordon Lonsdale and atom spy Klaus Fuchs. Generally, counterespionage cases are extremely difficult to prove in court because much of the evidence comes from sources too secret to be revealed and because MI5 is not a law-enforcement organization their main priority is to compromise espionage operations rather than focus upon prosecutions. As a result, cases against British citizens are relatively uncommon. When foreign nationals are involved, the tendency is to keep the case secret and deal with the suspected spy through diplomatic channels. One exception to this rule came in the 1970s when over a hundred Soviet diplomats were expelled from the United Kingdom in a single operation.

Government Communications Headquarters (GCHQ)

The third intelligence service in the United Kingdom is also by far the largest and most resource-intensive. The Government Communications Headquarters (GCHQ), based in a hi-tech doughnut-shaped installation near Cheltenham in the west of England, is responsible for intercepting and monitoring international and internal communications and collecting signals intelligence (SIGINT). GCHQ is the British equivalent to the American National Security Agency (NSA), which was founded in 1952 and under the authority of the Department of Defense. The collection of overseas communications by GCHQ is aided by a large number of listening posts, often in former colonial territories. The geographic coverage offered by the nations of the British Commonwealth and British possessions abroad is an important factor in the maintenance of the exceptionally close relationship with the United States. The first peacetime SIGINT agency was set up in the immediate aftermath of the World War I, in response to impressive successes by the Admiralty's Room 40 in intercepting German communications, including the notorious Zimmermann telegram. It was this agency, the Government Code and Cipher School (GC and CS), which was responsible for the most important and successful intelligence operation undertaken by British intelligence during the World War II, and it formed the basis for the postwar GCHQ.

The astonishing success of British code breakers, with vital assistance from their French and Polish allies, against the supposedly unbreakable German ENIGMA machine traffic was a crucial element in the fight against Hitler. Based

at Bletchley Park, a country house within the city limits of modern-day Milton Keynes, teams of linguists and mathematicians recruited directly from top universities, including Cambridge, regularly deciphered German communications, and this information was channelled to the relevant military, naval, and Royal Air Force (RAF) units. The contribution of this intelligence, code-named ULTRA, was critical to Britain's eventual victory in the Battle of the Atlantic, and it has been postulated that it shortened the war by at least two years. The phenomenal success of Bletchley Park was made possible by the innovative recruitment policies employed by GC and CS, which were the result of the World War I experience. The Admiralty's Room 40 had been staffed by a selection of Oxbridge professors, generally experts in the classical languages Latin and Greek, and they achieved notable success against German naval codes. Following this example the men in charge of Bletchley Park set out to recruit the best and the brightest. Recruiters were sent back to their old universities and tasked to choose exceptional candidates, regardless of age. Although the general feeling was that mathematicians were impractical eccentrics, several math students of particular genius were accepted. One of these was Alan Turing, who was to be one of the most important code breakers and the inventor of COLOSSUS, the first electronic computer.

SIGINT was also a major priority for British intelligence in the Cold War. Attempts to study GCHQ activities during that period are limited by secrecy regulations. The very existence of signals intelligence was for a long period a state secret and the policy of silence was strictly observed. Nonetheless, it is evident that the organization remains a critical part of the post–Cold War British intelligence community, and its relative importance is amply demonstrated by the fact that it has the largest budget. Most recently, SIGINT capabilities have been deployed, in cooperation with the United States, against terrorist targets and so-called rogue states, and are considered an essential element of the War on Terror.

Joint Intelligence Committee

Central to the workings of the intelligence community is the group of officials known as the Joint Intelligence Committee (the JIC). Developed during World War II, this interdepartmental body contains representatives of the three agencies, together with the Foreign Office and officials of the intelligence services of the army, navy, and air force (now grouped collectively in the Defence Intelligence Staff).[11] Its function is to assess and coordinate all intelligence so that government can be best informed as to the issues involved. The Committee is also responsible for coordinating intelligence for the Chiefs of Staff and, in addition, are tasked to consider any necessary steps that may improve the intelligence community as a whole. In the 1960s, the JIC was given its own staff, the Joint Intelligence Organisation, which prepares assessments for consideration

by the JIC and circulation to ministers.[12] Representatives of allied intelligence partners, particularly the United States, also regularly attend meetings of the JIC and receive the documents produced by the Committee. The establishment of the JIC as an independent body (though initially the Foreign Office provided the chairman), is one of the features of British intelligence that is praised most regularly in academic studies. The emphasis in the JIC is on consensus building, so that the policy makers do not receive contradictory reports which can hamper decision making.

Another advantageous feature of the JIC is its ability to form independent assessments of information, rather than coloring its analysis with its institutional influences. In this regard, it seems that the format of the British intelligence community has advantages over its American counterpart, where individual agencies have often competed rather than cooperated in providing intelligence assessments. The lack of a central coordinating body for all intelligence collected by U.S. agencies is a deficiency that all presidents since Truman have struggled to remedy. It is possible that the newly formed Director of National Intelligence and his staff may perform a comparable role, though it is too early to make confident predictions on this score.

The "Special Intelligence Relationship"

An essential element of British intelligence history since 1941 has been the close relationship between British and American intelligence organizations. It has been pointed out that behind the fraternal rhetoric, the most special element of the so-called special relationship between Britain and the United States is their intelligence collaboration.[13] Of all intelligence relationships this one comes closest to contradicting the statement of one Washington intelligence operative that, "there are no friendly [intelligence] services; there are only the [intelligence] services of friendly powers," and is testament to the close cooperation between the two nations. The unprecedented peacetime SIGINT alliance, enshrined in the UKUSA pact of 1947, has ensured that Britain has continued to be the most valued partner for the United States in the field of international intelligence.

This close nature of the relationship is a direct consequence of the experience of the two allies during World War II, in which successful collaboration and intelligence sharing made important contributions to various allied victories. Numerous senior American figures, including future President Dwight D. Eisenhower, were highly impressed by the British SIGINT capabilities. Ike, in his role of Supreme Allied Commander, described the contribution of ULTRA as being "of priceless value" and credited it with a major role in his successful landings in North Africa and Normandy. As well as the influence of the SIGINT achievements, individuals played an important role in supporting the development of a close postwar relationship. President Roosevelt's intelligence advisor William "Wild Bill" Donovan was a major supporter of collaboration with the British. This stemmed from the close relationship between Donovan and the SIS

representative in the western hemisphere, Sir William "Little Bill" Stephenson, and the inflated view propagated by Stephenson of British intelligence capabilities. Several figures in the American intelligence community felt that they gained much of their knowledge of intelligence matters from British experts. However, this interpretation has been questioned by some academics who point to a tradition of American intelligence going back to the time of George Washington.[14]

Regardless of the true nature of the British influence, it is evident that there was a feeling in Washington that the United States would gain from a close postwar relationship with its partners across the Atlantic, and this relationship has continued through various tumultuous and fractious events to the present day. Though the British were considered the senior partners during the war itself, the course of the early Cold War demonstrated plainly that Britain was no longer a "great power," and that she would now be the junior partner, albeit in a very exclusive alliance. The enduring nature of this relationship has been tested over the years, not least in relation to Soviet penetration of British intelligence, as discussed below, but it is a central feature of British intelligence history, and the signing of the UK-USA agreement in 1947 was a unique event in international relations.

The Cambridge Five

From the perspective of counterintelligence, one striking example demonstrates the unique history of the British intelligence community. As a case study, it involves the penetration by Soviet intelligence of the three wartime intelligence agencies and also demonstrates some of the strengths and weaknesses of the close intelligence collaboration between Britain and America. It is also a remarkable story of espionage and its potential contribution to international affairs and therefore serves as an excellent example of why the role of intelligence agencies is a subject that deserves academic attention.

Sir Richard Dearlove, former Director General of the Secret Intelligence Service, graduated in history from Queens' College, Cambridge University. Following his retirement in 2003 from his role as "C," he returned to Cambridge to take up a position as Master of Pembroke College, thus continuing the long connection between Britain's second-oldest university and the secret world of espionage. However, apart from the celebrated but fictional James Bond, the most famous Cambridge alumni in the intelligence world were the five Soviet agents recruited in the 1930s by the "Great Illegal," Arnold Deutsch.[15] Known as the "Magnificent Five" by their Soviet handlers, this quintet—John Cairncross, Donald Maclean, Kim Philby, Anthony Blunt, and Guy Burgess—all attained influential positions in the British civil service and intelligence agencies during World War II. The Five were not paid agents like CIA traitor Aldrich Ames, but instead were ideological communists who decided as young men to dedicate their lives to promoting the interests of international communism.

Their successes were remarkable. John Cairncross, the last of the Five to be identified, successfully attained positions that enabled him to report to the Soviets the two greatest secrets of the Allied war effort: first, in 1941, the fact that the British believed it possible to make an atomic bomb from uranium and were engaged in preliminary research, and second, from his later role as a linguist at Bletchley Park, that the British were reading German encrypted messages. Information he passed to his handler while at GC and CS, the forerunner to GCHQ, is regarded as central to the Soviet victory in the battle of Kursk, the biggest tank battle in history and one of the major turning points of the war.

His success, though notable, is, however, overshadowed by that of Kim Philby, who was recruited into SIS Section V (counterespionage) shortly after the outbreak of war. As the war drew to a close, Philby managed to secure his appointment as head of a newly formed anti-Soviet branch, Section IX, from where he was able to pass information to the KGB about all operations and SIS agents in the Eastern Bloc, and directly compromise joint SIS/CIA missions in Albania and the Baltic states. His final coup was to secure himself the role of SIS Head of Station in Washington, DC, a central position in the transatlantic alliance. This senior appointment has been taken as evidence that he was being groomed as a future "C," the Director General of the SIS. Certainly, the Washington post was one of the most important in the organization, and it was in this position that he was able to keep the Soviets informed of CIA operations against them, and equally importantly, about the VENONA project that was identifying Soviet spies in the United States. The access Philby had in Washington is remarkable, and made all the more so by the fact that the FBI considered him and his British colleagues as more trustworthy than their foreign intelligence counterparts at the CIA, who were not even informed of VENONA's existence.

As Philby was enjoying his meteoric rise at the SIS, his Cambridge contemporary and friend Donald Maclean was making comparable progress at the Foreign Office.[16] The son of a former Cabinet minister, Maclean had both the personal characteristics and, crucially, the right background to succeed as a diplomat. As well as serving as First Secretary in the Washington embassy, Maclean headed the American desk in Whitehall upon the outbreak of the Korean War. A dedicated communist since his university days, he was able to pass enormous volumes of classified information to the Soviets, including verbatim transcripts of messages sent between Winston Churchill and Franklin D. Roosevelt. Both Burgess and Blunt, though less spectacular in their achievements, played key roles in the ring. Burgess recruited Philby into the SIS and later worked in the Foreign Office, while Blunt used his position as a junior fellow at Cambridge to talent-spot other potential Soviet spies, as well as serving in MI5 himself during the war.[17]

The activities of the group were at last detected after the code-breaking project VENONA produced evidence of a Soviet spy in the British embassy in Washington. Although the CIA was kept in the dark about VENONA until 1952, as a result of the intelligence relationship between the British and Americans

Philby was fully indoctrinated and was therefore able to monitor progress on the decrypts. The list of suspects was gradually narrowed down, until Maclean was identified as the only possible candidate. Thanks to his role in Washington, Philby was able to warn Maclean that he was to be arrested, and he defected to the Soviet Union in the company of Burgess in 1951. This put Philby under suspicion, because Burgess had been his lodger while working at the British Embassy in Washington. Philby was forced from Washington by the Americans and investigated by MI5, while press reports referred to the mystery of the "Third Man," a phrase made famous by the Graham Greene book of the same name. However, no concrete evidence was uncovered against him and, though he lost his job at the SIS, he never faced trial. Continuing to protest his innocence for some time after the defection of his university contemporaries, Burgess and Maclean, he even set up a press conference in his mother's flat in 1955 in response to allegations made about him in the House of Commons. In 1963, after confessing his involvement with the KGB to a former colleague, he defected to Moscow from Beirut, where he had been working as a journalist.

Neither of the other two members of the ring were ever prosecuted for their involvement in espionage, although Cairncross was fired from the civil service and advised by MI5 to leave the country after a note in his handwriting was found in Burgess's apartment. Blunt had a very successful career as an art historian and became Keeper of the Queen's Pictures, a highly prestigious post in the royal household. Though he admitted his involvement in Soviet espionage in 1964, he was given immunity from prosecution. Eventually he was exposed as the "Fourth Man," after the publication of Anthony Boyle's *A Climate of Treason* in 1979, and stripped of his knighthood.

This episode, a highly popular subject for undergraduates at Cambridge, is an extraordinary illustration of the scale of the Soviet espionage assault on the United Kingdom. It has also been the source of great controversy, and it placed the British-American intelligence relationship under exceptional strain, as well as dividing MI5, who were convinced that Philby was guilty, from MI6, who sought to protect their former officer.

THE SOURCES

There are two major sources for writing about British intelligence, and both present major problems to the historian. First, there are official documents that record the activity and organization of the British intelligence agencies; these include both the documents of the agencies themselves and the records of the government departments that receive their output or monitor their expenditure. The last few years have seen major changes in the release policies of the intelligence agencies, though the progress is uneven and limited by the need to balance openness with security concerns. The second major source is the personal accounts of former members of those organizations and those who were informed of

their activities (for example, politicians), both in the form of oral testimony and in written memoirs. Any references to intelligence by either group are heavily discouraged by the British establishment, who hold on to the notion that the potential risk to security offsets the benefit to historical understanding. Nonetheless, the recent moves toward greater openness, at least in relation to archives, are a welcome boon for students of intelligence, and the decision to allow a former Director General of MI5 to publish an autobiography in 2001 demonstrates some degree of flexibility in relation to intelligence-related memoirs.[18]

Official Documents

Professor Christopher Andrew has identified two major prewar constitutional principles that established the precedent for the treatment of intelligence issues by public figures: "that intelligence is undiscussable in public and that parliament surrenders all its powers in intelligence matters to the executive."[19] These principles were expressed directly by Foreign Secretary Austen Chamberlain in November 1924, in the House of Commons: "It is the essence of a Secret Service that it must be secret, and if you once begin disclosure it is perfectly obvious to me as to hon. Members opposite that there is no longer any Secret Service and that you must do without it."[20]

The philosophy that the only alternative to total secrecy is complete exposure is no longer held to be adequate in a democratic society in which intelligence services are seen to play an increasingly important role. However, it conditioned the attitude of a succession of British governments of both major parties toward intelligence until two decades ago. Many commentators believe that the drivers of this policy of excessive secrecy are the agencies themselves, and that the government's acceptance of their need for secrecy has been to a large extent unquestioning. Several reasons have been advanced to explain the longevity of this policy, generally centering on bureaucratic impulses to protect information and to preempt inquiry. As a consequence, historians hoping to write documented accounts of intelligence-related events have been heavily restricted in what files they can access, and this state of affairs has generated some disquiet in the media and academic community over the notion that government files are being retained without due cause.

The charge of excessive caution is refuted by the intelligence agencies when they seek to justify the continued retention of their archives. They base their arguments against declassification on the issue of operational effectiveness. They identify two key areas of their activity that might be jeopardized by greater openness: recruitment of agents and intelligence-collection methods. The agencies claim, with some justification, that the trust that is so essential for the recruitment of sources of intelligence would be adversely affected if potential spies knew that their identities and the nature of their espionage might become public knowledge. They point out that the need for secrecy has no specific lifespan, as publicizing an individual's involvement in espionage can prove dangerous for their descendants, who may find their own lives in jeopardy on

account of the activities of members of their family in previous generations. Moreover, it is widely felt that the methods that are used in both technical intelligence collection, for example by GCHQ, and for handling agents, by the SIS, might become known to potential enemies, who would therefore take preventive action.

The prevailing view in the SIS is that their archives should never be made public, even if the material predates World War I. The principle of protection of secrecy and the dangers of the so-called slippery slope are regarded as ample justification for this blanket policy of retention. The legislation behind the retention of files has been subject to periodical reviews, a process summarized below.

Legislation on public records in 1958 and 1967 required government departments to safeguard a proportion of their files. Strict criteria are used to decide which files can be destroyed and which must be preserved for future reference and eventual release. The 1958 Public Records Act's provisions laid down a fifty-year limit after which documents should be moved into the public domain, a period that was subsequently reduced to thirty years in 1967. Though the three intelligence agencies were required to keep their documents in their own archives, Section 3(4) of the Act allowed the Lord Chancellor to exempt files relating to certain subjects from the release requirements. All files related to intelligence and the intelligence services were granted a so-called blanket exemption, meaning that the agencies were not required to release any of their archives, even after the thirty-year period had elapsed. The consequence of this decision was that all intelligence files were retained by the agencies. This initial "blanket," which covered all security and intelligence records, was subject to re-examination after intervals of twenty-five years. This was in line with the established official view of intelligence, reaffirmed after World War II, that the activities of the intelligence agencies should never be publicly acknowledged and that their files should remain under departmental control indefinitely. Though the blanket was not compulsory, meaning that the agencies could release any files if they so wished, perhaps predictably they opted to continue their traditional reticence.

"NEVER-NEVER LAND"

In 1982, the Parliamentary Committee on Modern Public Records (the Wilson Committee), reconsidered the public records legislation and consulted with the relevant government departments. They were given "categorical assurance" that the security agencies were complying fully with this legislation, and that their archivists were systematically collecting and storing the required files. Also, in a departure from the accepted view that intelligence documents should never be released, the Committee's white paper argued successfully that, in relation to declassification, "the word never should never be used." This phrase led Canadian intelligence historian Wesley Wark to claim memorably that the archives were existing in "Never-Never Land."[21] The committee further concluded that "ultimately the government of the day will find it possible to release these records—say

by the time they are 75 years old—although we recognize that in some cases retention may continue to be necessary for 100 years, or possibly even longer." Therefore the principle of eventual release was affirmed, even if, as one British intelligence historian has said, this might be in a "far off place."[22] Nonetheless, it was a step toward greater openness and was backed up by a decision to re-evaluate the case for the renewal of the blanket order on a more frequent basis.

Somewhat ironically, events overseas played a role in provoking a re-examination of this policy. The results of the 1975 Church Commission's investigation into the American intelligence community and the establishment of the Senate and House Committees on intelligence during that decade rendered study of the role of intelligence in U.S. foreign policy more accessible and led to some pressure for comparable action in the United Kingdom. Moreover, the existence since the 1970s of the Freedom of Information Act (FOIA) in the United States meant that there was more archival material available on British intelligence in the American government archives than there was in the British Public Records Office. This seemingly paradoxical situation was evident in the historical treatment of the case of Soviet atom spy Klaus Fuchs, the subject of two biographies published in 1987, both of which drew extensively on FBI files based on MI5 material.[23] In order to learn about MI5 counterespionage activities against a British spy, scholars had to visit an archive in the United States. Similarly, the FBI files on the British-born Soviet spies Kim Philby, Donald Maclean, and Guy Burgess, all of whom spent time based in Washington, were released in the 1980s, but to this day they remain classified in the United Kingdom.[24]

In the late 1980s and early 1990s, a new pressure for openness emerged from an unexpected source. In the period of *Glasnost*, and in the immediate aftermath of the end of the Soviet state, there was a temporary easing of the restrictions surrounding Moscow's intelligence archives, which allowed some Western historians access to intelligence material, albeit with certain restrictions.[25] In addition, several former Soviet spymasters published memoirs discussing their operations in the West, including Britain.[26] It seemed to many observers that one could learn more about British intelligence operations from the other side than from the British government. These episodes, together with the damage to the image of British government caused by a series of intelligence scandals, helped create pressure for a greater degree of transparency in relation to intelligence.

OPEN GOVERNMENT INITIATIVE

In 1993, the issue of government secrecy was re-examined by the then-Chancellor of the Duchy of Lancaster, William Waldegrave. The consequence of this inquiry was the Open Government Initiative, which strengthened the role of the Lord Chancellor's Advisory Council on Public Records and gave the members of the Council access to all applications for the retention of documents. It also allowed independent historians to participate in the process of reviewing documents for release.[27] Though the existence of regulations allowing for blanket

retention was not challenged, the Initiative is credited with encouraging a greater degree of openness. Over the same period, new legislation was enacted relating to the intelligence services, which for the first time placed the agencies on a statutory basis. (The Security Service Acts of 1989 and 1996 related to MI5; the Intelligence Services Act 1994 related to SIS and GCHQ.) This legislation, the Waldegrave initiative, and the increasing recognition by the intelligence agencies that the world in which they operate is changing rapidly, have all contributed to a degree of openness that a generation earlier would have appeared unthinkable.

The most recent development in terms of access to government files has been the passage of Freedom of Information legislation in the United Kingdom. Though this is similar in principle to the American FOIA, in Britain the files of the three major intelligence agencies are explicitly excluded from its statutes. Nonetheless, though there is no compulsion, some of the principles behind the legislation have been adopted by MI5 in their recent voluntary declassification program. Sir Stephen Lander, until 2001 the Director General of the Security Service, perhaps reflecting his own background as a Cambridge history student, declared that he and MI5 regarded "intelligence records as public records."[28] In keeping with this principle, the last five years have seen an unprecedented policy of declassification of intelligence documents. MI5 has been most prominent in this program, declassifying much of their pre-1945 archives, along the lines laid out by the Advisory Committee. GCHQ has also released further World War II material, including decrypted messages from Bletchley Park. The Secret Intelligence Service, though retaining all of its own archive, has declassified large sections of the files of the wartime organization, the Special Operations Executive (SOE), for which it has responsibility, and has allowed the release of SIS documents held in the files of other departments. This represents a major shift in policy and one that has had positive consequences for the historical study of British intelligence.

In spite of the greater degree of openness in recent years, including the appointment of an official historian, it is important to remember that the policy is selective and partial. Virtually all British intelligence historians who rely on declassified documents have had to contend with the frustration caused by the occasional retention or sanitation of a desired file. Further secrets, particularly related to more recent events, remain classified, and there is no prospect of the SIS declassifying any of their archive in the near future. Nonetheless, the declassification program should be welcomed as a step in the right direction and presents an unprecedented opportunity for British intelligence historians.

MEMOIRS AND ORAL HISTORY

Historian Richard Aldrich has pointed out that scholars should retain a degree of skepticism when faced with files that have been through a process of official vetting. In an article in *Intelligence and National Security* he cautioned his colleagues not to become reliant on what he terms, "the processed food available in the PRO's (Public Record Office) history supermarket," limited as it

is by a "pre-selected menu," and advises them to "grow their own" intelligence material by supplementing their archival research with interviews and alternative sources.[29] Unfortunately, researchers are confronted with problems caused by the government's release policies and official legislation. Frequently, historians are denied the opportunity to supplement their archival research with information from memoirs and interviews. There are two issues involved in this question: first, the fact that the law, specifically the Official Secrets' Act, prohibits government employees from discussing classified information, and second, the seemingly excessive time delay before government documents are released into the public domain. These restrictions, though ostensibly prompted by security concerns, are a hindrance to historical research and represent an area in which the British intelligence community can learn from the American experience. Though the United States is also conscious of the need to protect intelligence methods, there is some recognition of the need for flexibility when dealing with former employees who wish to write or comment on their experiences and who can make vital personal contributions to the historian's study of intelligence.

From a personal perspective, my own research has been greatly aided by FBI Supervisor Robert Lamphere's 1986 book *The FBI-KGB War*. Lamphere, who worked as FBI liaison on the VENONA project, conducted the investigations into the Rosenbergs and Justice Department employee Judith Coplon, among others. His first-hand account discusses the role of the decryption program in counterespionage operations in general terms, relating it particularly to his investigations into atomic espionage, culminating in the Rosenberg case. It is a particularly valuable source and provides many insights into the mentality at the FBI in the 1950s, as well as describing the investigations from the perspective of a major participant. With the support of the Bureau, Lamphere overcame some opposition from the National Security Agency and submitted his manuscript for clearance through established channels. Minor alterations were requested and accepted by the author, and the book was published in 1986. No comparable history has been written by any British investigator from MI5, and any attempt to publish such an account would almost certainly bring a vigorous response from the government. Though the events in question occurred in the 1940s and 1950s, the emphasis in Britain is on secrecy rather than openness, particularly in relation to signals intelligence.

The dearth of intelligence memoirs in Britain is due both to the culture of secrecy that prevails in British intelligence and to government legislation designed to prevent former officers from writing or talking directly about their experiences. The Official Secrets' Act is the legislation most commonly used to gag former intelligence professionals. In 1989, partly in response to the publication of Peter Wright's memoir *Spycatcher*, the Official Secrets' Act was rewritten with specific reference to the intelligence community. It explicitly prohibited "all intelligence officers from disclosing any aspect of their service, irrespective of its nature or when it took place," and was retrospectively applied. Nigel West, an author whose books have relied on a fair proportion of "insider" information, has bemoaned the restrictive nature of the legislation:

> To obtain a conviction under the new law, enacted in 1990, the Crown was required merely to demonstrate that an individual who was, or who had once been, employed by the security or intelligence services, had revealed information. The issue of whether the data was already in the public domain, or perhaps was of a trivial nature, was deemed irrelevant.[30]

The most recent intelligence case under this new Act concerned the recollections of former junior MI5 officer David Shayler, which resulted in a warrant for his arrest. Shayler, a paunchy and unimpressive-looking figure, featured in several articles in the *Mail on Sunday*, beginning with a front-page story on 24 August 1997 under the headline "MI5 bugged Mandelson." The story referred to the claim that the Security Service had eavesdropped on the telephone calls of the one-time Northern Ireland Secretary and current European Trade Commissioner in the 1970s. Embarrassing though Shayler's revelations were, the damage done to current operations is limited compared with the aftermath of the publication of former CIA agent Philip Agee's highly critical account *Inside the Company: CIA Diary*. Agee, disgruntled with his treatment by the Agency, named many hundreds of CIA agents working under official cover abroad, an action that had tragic consequences when an operative identified by the renegade agent was assassinated in Athens.[31]

Nonetheless, there have been occasional exceptions on the British side. In contrast to the Shayler case, former Director General of the Security Service Dame Stella Rimington was permitted to publish her autobiography in 2001, although she faced considerable opposition from within Whitehall and her own organization. The manuscript was subjected to vigorous scrutiny, and any suggested omissions were accepted by the author. The comments on the back cover of the paperback edition demonstrate conclusively that the debate over intelligence memoirs is still fierce; the *Daily Telegraph*, a generally conservative paper, supported her right to publish emphatically, describing it as "vital in stripping away mystique and building understanding." Conversely, Margaret Thatcher's former Press Secretary Sir Bernard Ingham slammed Rimington, while unconsciously echoing Chamberlain's statement from the 1920s, "The most effective Secret Service is one which is secret. She should shut up."[32] Rather than setting up an approved vetting channel for the publication of memoirs, as exists in the United States, the British government, though it relented in the case of Rimington, remains firmly opposed to the principle of publication by former intelligence officers, a decision that cannot help either historical understanding or their own attempts to render their activities more transparent.

The second obstacle for the use of first-hand accounts in research is equally frustrating. Once information is in the public domain, former intelligence officers are permitted to discuss it in interviews with academics or in their own memoirs, subject to agreed protocol. However, the general tendency is to retain intelligence documents well beyond the thirty-year point. This can have the unfortunate consequence that the people whose actions are recorded in the documents are no longer alive to discuss them. As mentioned earlier, the decision to release files that

have been retained beyond their normal release date by government departments is reviewed periodically by the Lord Chancellor's Advisory Committee. They have the opportunity to recommend the release of documents when they review the conditions of the blanket every ten years. Though it is accepted by historians that the Committee need to exercise restraint in relation to official documents, some of their decisions can be difficult to understand on security grounds. For example, the decision to retain SOE records for fifty years has meant that few of those with first-hand experience are still in a position to share their memories with historians, contrasting unfavorably with the decision by the American intelligence community in the 1980s to release files relating to the activity of the OSS.[33]

In relation to the atom spies, the decision to declassify VENONA in 1995 allowed academics to interview Theodore Hall, who at age 19 had become the youngest spy in the KGB's history. Hall was not publicly identified as a Soviet agent until copies of the cables were released, because the only evidence against him had been provided by signals intelligence. The declassification of the cables demonstrated his involvement in espionage, and before he died in 1997 he was able to give his side of the story to several different commentators. Though it was a project on which GCHQ collaborated, the British agency's files on VENONA are almost all retained, with no projected date for declassification, leaving scholars to speculate as to their contents. Fortunately, the decrypts related to Britain were released by the NSA, but when the VENONA files themselves are declassified, it is unlikely that any of the participants will be alive to discuss them, whereas in the American case several of the major code breakers, including the legendary Meredith Gardner, have been able to speak of their experiences in interviews. The hope must be that the British policy of declassification will speed up so that other opportunities are not missed due to the passage of time.

In general, the trend toward openness is one that should continue in the longer term, and this can only serve to benefit historians. Some delays and problems are inevitable, but a cooperative attitude on both sides is likely to mitigate some of the difficulties presented by the issues of security and secrecy. Though government policies on this issue have been somewhat out of step with contemporary thinking, the rapid pace of recent progress demonstrates that when the prevailing view of Whitehall is challenged, impressive results can follow. In relation to memoirs, the potential lesson from the American experience is that when the correct procedures are adhered to, allowing intelligence officers to speak about their experiences, or publish memoirs, can greatly enhance historical understanding and serve as an essential tool for supplementing archival research.

WRITING ABOUT BRITISH INTELLIGENCE IN THE POSTWAR PERIOD

It is over twenty years since the publication of *The Missing Dimension*, a collection of essays on intelligence edited by Professor David Dilks and Christopher

Andrew. In the introduction, the editors drew attention to the fact that academic historians have tended to shy away from addressing issues relating to intelligence and that this deficiency can result in a distortion of historical understanding. They postulated that the problem of availability of sources on intelligence was compounded by a general academic distaste for the subject, prompted by the "evident absurdity of many best-selling publications on the subject," a trend that they identified as predating World War I and continuing into the present day.[34] However, many books have been written about British intelligence over the last century, although their quality and documentary basis has frequently fallen short of academic standards.

After World War II, the view of the British civil service was that the secrecy of the intelligence used to such great effect in that conflict had to be protected. In fact, the government consciously sought to mislead historians and the public as to the role of intelligence during the war by a deliberate policy of obfuscation. When official historians were appointed to chronicle the course of the conflict, they were indoctrinated into the secrets of ULTRA and the strategic deception, and were then instructed to omit all mention of their contribution from their histories. They were particularly concerned during the 1950s, when files from inside Germany and Italy threatened to betray the secrets of ULTRA. Comparison of Axis files with British orders would, it was believed, reveal that the Allies must have been reading the enemy's communications.[35] However, contrary to their expectations, the first generation of independent World War II historians accepted the government line without much comment, therefore protecting the secret of ULTRA.

Whitehall's case was aided by the fact that the author of the most widely read history of World War II required little in the way of instruction. Winston Churchill's six-volume memoir set an important precedent by telling a version of the war that made almost no mention of the use of SIGINT.[36] Churchill, a great SIGINT enthusiast, was painfully aware that future operations might be jeopardized by any public confirmation of their existence, and with some assistance, managed to restrain himself from damaging references. His awareness of the risks involved stemmed from his disastrous decision, while Home Secretary in 1927, to make public a decrypted Soviet message for political purposes. This revelation led Moscow to change their encryption method to the theoretically unbreakable one-time pad system, thus robbing the British government of their best source of intelligence on the Soviet Union.

For almost thirty years, the ULTRA secret was protected—a remarkable fact considering that thousands of people had been involved with Bletchley Park. However, in the 1970s, the truth began to emerge, provoking much debate both in Whitehall and in academia. The threat to the secrecy of ULTRA and the "double cross system" came not from investigative historians but from former senior participants who wished to record their version of events.[37] The most important of these insiders was an Oxford academic, J. C. Masterman, the former Chair of the XX Committee that had overseen the double cross system. As well as

enhancing historical understanding, Masterman, in the preface to his account, alluded to two other major motivations:

> It is also right to give credit for a successful operation to those who deserved it. . . . This I took to be important because the opinion of the Secret Service was so low. Any good work done by the Secret Service is usually unknown except to those in high places and those personally concerned. On the other hand any error or partial failure receives a great deal of publicity and a spate of criticism.[38]

At the time of publication in 1972, the image of British intelligence, already damaged by the defections of the three Cambridge spies Burgess, Maclean, and Philby, was under further attack due to the negative presentation of the SIS by Philby in his memoir, *My Silent War*, published in 1968. Masterman, then in his eighties and with exceptional social connections, had little to fear from the establishment. He resolved to publish his informed account both to pre-empt any lesser works and to publicize the success and innovation of the system. This double line of reasoning was also employed by the National Security Agency and the CIA when they declassified material relating to the VENONA project in 1995. Hundreds of NSA employees had contributed to this ground-breaking and extraordinary endeavor, and were being denied recognition for their exceptional achievements. Publication in 1995 also allowed several of the key participants to be interviewed by historians about their contributions and experiences. It also helped offset criticism aimed at the American intelligence community over the discovery that CIA officer Aldrich Ames had been a member of the KGB since the 1980s.[39]

Two years after Masterman, a second insider, Group Captain Frederick Winterbotham, published *The ULTRA Secret*, and Churchill's "Goose That Laid the Golden Eggs" was unveiled. In response, the government decided to publish a new series of official history, this time concentrating on the role of intelligence during World War II. A team of historians was appointed, headed by Sir Harry Hinsley, a veteran of Bletchley Park and Master of St. John's College, Cambridge. Hinsley's five-volume series was written with "unrestricted access to the intelligence records for the inter-war years and the Second World War, as well as to other relevant archives."[40] The first two volumes were published in 1979 and 1981, and the third in 1988. At last, there was some degree of acceptance of a need to enhance public understanding of the contribution of intelligence to the Allied victory. Although they had been ready for publication a decade earlier, the contents of the last two volumes, on counterintelligence and strategic deception, were deemed too sensitive and consequently these volumes, by Michael Howard and C. G. Simkins, were not published until 1990. The experience of ULTRA veterans demonstrates some of the benefits of declassification. Following the decision to remove the veil of secrecy around the decipherment program, former code breakers were at last allowed to make reference to their wartime activities. A reunion was held at Bletchley Park in the summer of 1991, allowing former colleagues to be reunited and to discuss their activities with assembled historians.

For many of the participants, this was the first time they had been able fully to understand the role that they had played in the extraordinary success against the German ENIGMA machine. They also used this opportunity successfully to lobby the government to step in to preserve the site and set up a museum on cryptology and computer science, in view of the contribution of Bletchley Park to both the Allied victory and the development of electronic computing.[41]

It has been clear that many historians have failed to apply the lessons of the ULTRA secret to other contexts; for example, most Cold War histories do not mention the potential contribution of SIGINT. This demonstrates a major limitation that has constrained the development of a tradition of Cold War history that takes into account the intelligence dimension; most historians struggle to deal with concepts that are unfamiliar and that they are not accustomed to viewing as important.[42]

In conjunction with this general tendency to underrate the contribution of intelligence, the dearth of available documents further discouraged most academics.[43] As a result, the late 1970s and 1980s were dominated not by academic investigations into British intelligence but by sensationalist accounts of intelligence agencies by authors relying on "inside" information. Encouraged by the memoirs of Kim Philby and the exploits of SIS spy and KGB mole George Blake (another Cambridge graduate), the dominant theme of much of this writing was mole-hunting, similar to that witnessed in the United States as a result of the work of former CIA Counterintelligence Chief James Angleton.[44] The development of this brand of "airport bookshop" accounts can be viewed as an unintended consequence of the obsessive secrecy surrounding intelligence-related material in the United Kingdom.[45] This literary trend has been given further impetus by the British public's seemingly insatiable appetite for investigative exposés of the intelligence community, encouraged by revelations about the Cambridge Five. Philby's defection in 1963 had sparked a newspaper debate over the identity of the so-called Fourth Man, a notion encouraged by sporadic leaks to the press by anonymous sources in the intelligence community. The publication of Anthony Boyle's *A Climate of Treason* in 1979 forced Prime Minister Margaret Thatcher to confirm that in a 1964 statement Sir Anthony Blunt had admitted being a Soviet agent. With the issue of the "Fourth Man" now settled, the search moved on to the identity of a "Fifth Man," and a fresh round of mole-hunts began.

In the 1980s, at the same time that some serious academics were beginning to address the intelligence dimension, the search for Soviet spies reached new extremes. Journalist Chapman Pincher, acting on information from MI5's Peter Wright and MI6's Arthur Martin, laid the blame for the clearance of atom spy Klaus Fuchs squarely at the door of the former Director General of MI5 Sir Roger Hollis, whom he accused of being a Soviet agent.[46] In response to a Parliamentary Question, the Prime Minister was forced to admit that Hollis had indeed been investigated as a potential mole, but cleared. With the benefit of recently declassified files, the public can now check this conclusion for themselves, and on examination Hollis emerges as no more culpable for the successive clearing of Fuchs than several of his colleagues. This episode demonstrates some of the

benefits of declassifying documents rather than allowing conspiracy theory to occupy the information vacuum created by government secrecy, but it also highlights the turbulent and sensationalist nature of many accounts of British intelligence, particularly in relation to Soviet espionage.

The conflict over official secrecy came to a head in 1986 with an extensive court battle in Australia between Peter Wright and the British government over the publication of his memoir *Spycatcher*. In the book, Wright, a former Assistant Director at MI5, railed against the Service for what he perceived as their failure to act against moles inside the organization. The severity of the British government's response generated enormous publicity for Wright and greatly increased the sales of the account. The court case in Sydney, which accused Wright of breaching confidentiality agreements, was remarkable for the admission by the then-Cabinet Secretary, Sir Robert Armstrong, that he could not admit SIS exists in peacetime, and that on occasion civil servants found it necessary to be "economical with the truth." As well as encouraging the government to place the intelligence services on a firmer statutory basis through legislation like the Security Service Act (1989), the *Spycatcher* case was a driving force behind the revision of the Official Secrets' legislation, and demonstrated that the British government remained opposed to the publication of intelligence memoirs.

Happily, the late 1980s and early 1990s saw the study of intelligence move toward acceptability in British academia, and a proliferation in the number of courses in intelligence history.[47] However, it is with the development of this school of "intelligence historians" that the final common problem with academic writing about intelligence in Britain becomes more of a cause for concern. This is the overemphasis on the minutiae of the intelligence institutions themselves, rather than examining their activities within a broader contextual framework.[48] This tendency has been identified by John Lewis Gaddis, who challenged intelligence historians to illustrate more clearly the extent to which secret activities actually influence world events, rather than adding to the existing literature of organizational studies. As long as historians are mindful of the need to retain a broader sense of perspective, the growing availability of new intelligence documents cannot fail to continue the development of the discipline. Moreover, other specialists in international relations, diplomatic history, and politics can use these studies to enhance their own work and ensure that the intelligence dimension is no longer overlooked.

AN OFFICIAL HISTORIAN FOR THE CENTENARY

As part of their efforts for a greater degree of openness, in 2001 MI5 appointed Cambridge University Professor Christopher Andrew as their first official historian. He has been commissioned to write the Centenary History of the Service, due for publication in 2009. As well as being granted unprecedented access to files, Andrew will conduct extensive interviews with former and current officers of the Service. He has identified three criteria that official historians

of intelligence must follow, and that he has ensured will be guaranteed by his employers: First, official histories should be based on full access to files; second, the historians should have "complete freedom to reach whatever conclusions they believe are consistent with the evidence"; last, official historians must deal with the interactions of intelligence with policy makers, not just intelligence itself.[49]

However, some in the academic community have reservations as to the propriety of appointing official historians. Brunel University Professor Anthony Glees, once considered as a candidate for the job, has commented: "It is a principle of a free society that the people who write its history should be entirely free and unfettered. I don't think governments should write their own history. Academics should not become ambassadors or politicians, or work for the secret services."[50]

Other historians have suggested that Professor Andrew occupies the post of "court historian" for the intelligence services because they have twice employed him to cowrite histories of the KGB with the help of Soviet defectors Vasili Mitrokhin and Oleg Gordievsky.[51] However, Andrew has responded to these criticisms by pointing out that the files he uses will eventually find their way into the public domain and that he therefore has his academic reputation to consider. He has been supported both by Richard Evans, who points to his Cambridge colleague's record of professionalism and accuracy, and fellow intelligence historian Richard Aldrich, who has commented that the risks of white-washing and cover-ups are mitigated because intelligence historians, of whom there are now more than fifty in the United Kingdom, are trained to be skeptical of official documents.[52]

Following the example set by MI5, the Foreign Secretary recently sanctioned the appointment of Keith Jeffrey of Queen's University, Belfast, to write another official history of the organization from 1909 to the early Cold War. Jeffrey will have unlimited access to the SIS archive, although given the importance of confidentiality to the SIS's work, he will not name individuals or refer to potentially sensitive operational details.[53] Nonetheless, there are limits to the program of openness and debate, because there is no such prospect of parallel research by independent historians as is made possible for the first fifty years of MI5 (thanks to the declassification program), since the SIS archives will remain classified. Moreover, despite the trend toward a greater openness, there is nothing comparable to the CIA's Center for the Study of Intelligence in the United Kingdom. This program, directed by Paul Johnson, brings together the Agency's analysts, operatives, and administrators, together with historians, to author studies of the Agency's performance, which are then released in classified and declassified versions.[54] Furthermore, the CIA allows its analysts to write articles in other academic journals, while several former Directors of Central Intelligence and some less senior officers have published approved and well-received autobiographies. Despite the public use of JIC material in the recent Iraqi debates, the intelligence services in the United Kingdom have yet to publish any thematic collections of intelligence documents along the lines of the CIA documents on the Cuban Missile Crisis or the NSA publication on the VENONA project. This may partly reflect the fact that unlike the Agency's Directorate of Intelligence, SIS, GCHQ, and MI5 do not

produce finished intelligence analysis along the lines of the American National Intelligence Estimates. However, despite these contrasts, it is clear that the American intelligence community is not uniformly convinced as to the benefits of self-examination through historical research. Indeed, the FBI has only relatively recently appointed John Fox as their in-house historian, after a gap of almost a decade, and the Bureau's attitude toward historical research is somewhat ambiguous.

In its mission statement, the CIA's Center for the Study of Intelligence (CSI) includes a commitment to the encouragement and improvement of the teaching of intelligence. For example, an American professor at a large public university in the United States recently took a sabbatical to teach at Yale University. As he was an expert on intelligence, his replacement had to be familiar with the topic. Instead of appointing another academic, the university appointed a serving officer of the CIA to teach the required courses, in collaboration with CSI. Though the British intelligence community has not yet acquired this degree of openness, there have been several positive developments in the relationship between academia and the "secret world," with recent speakers at Cambridge University events including the current Director General of MI5, Dame Eliza Manningham-Buller, and her predecessor Sir Stephen Lander. In addition, the current Master of Pembroke College, Sir Richard Dearlove, has twice presented to the Cambridge Intelligence Seminar on his work as Director General of the Secret Intelligence Service. In spite of this progress toward greater openness, it will be many years before the SIS will follow the CIA's example and allow an academic anthropologist inside their organization to study their working procedures and comment on them to students at a foreign university.[55] Perhaps this is a pity.

CONCLUSION

On a positive note, the idea that intelligence is the "missing dimension" of historical writing is no longer as valid as it was twenty years ago. A generation of historians has grown accustomed to making reference to the work of secret services, most notably in relation to World War II, and with the growing availability of Cold War materials it is hoped that this trend will continue. Moreover, in an era in which intelligence is more widely discussed and used than ever before, and is the explicit basis for certain foreign policy decisions, it is evident that this British tradition of intelligence-centered history must endure. Certainly, if the popularity of intelligence-related courses at both undergraduate and graduate level is any sort of measure, then the subject is attracting unprecedented levels of interest. Nonetheless, there is the risk that those who study intelligence will fail to understand that the intelligence services do not act in a vacuum. They are the tools of government and, as such, should be studied in their correct context. The debate over availability of sources can condition a brand of intelligence history that focuses too tightly on the agencies themselves, instead of relating their activities to the policies of the government they served.

Though the current climate of encouragement of openness is a refreshing change from the extreme secrecy of the past, the uneven nature of the declassification and the draconian restrictions on what former operatives can say or write about their experience continue to provide obstacles that block true understanding. The appointment of an Official Historian for MI5 is a welcome step, as is the commissioning of an official history for the first fifty years of the Secret Intelligence Service. Consequently, the present era is an exciting time to be a student of British intelligence, and if current trends continue, the prospects for the next generation of historians appear even more promising.

NOTES

1. Professor Peter Hennessey of Queen Mary and Westfield College, University of London, used the phrase as the title for the Harry Hinsley Lecture on intelligence at St. John's College, Cambridge University, in November 2005.

2. The Secret Intelligent Service was never known as MI6, though during World War I it was designated Military Intelligence 1C (abbreviated to MI1C). The name MI6 has been erroneously used so often that it has entered common parlance.

3. C. M. Andrew, *Secret Service: The Making of the British Intelligence Community* (London: Heinemann, 1985), p. 318.

4. The sting operation was carried out by the Combined State Political Directorate or Obyedinyonnoye gosudarstvennoye politicheskoye upravleniye (OGPU), a precursor to the KGB, the Soviet intelligence organization.

5. P. S. Deriabin and J. L. Schecter, *The Spy Who Saved the World* (New York: Random House, 1988).

6. C. M. Andrew and V. Mitrokhin, *The Mitrokhin Archive: The KGB in Russia and the West* (London: Penguin, 2000); C. M. Andrew and O. Gordievsky, *KGB: The Inside Story of Its Foreign Operations From Lenin to Gorbachev*, 2nd ed. (London: Sceptre, 1991).

7. The idea that the Germans were conducting espionage operations in Britain was encouraged by popular literature and the press.

8. Broadcast in Britain under the title "Spooks."

9. The Abwehr was the German intelligence organization headed by Admiral Canaris.

10. F. H. Hinsley and C. A. G. Simkins, *British Intelligence in the Second World War. Vol. IV: Security and Counter-intelligence* (London: Her Majesty's Stationary Office, 1990), p. 87.

11. The Defence Intelligence Staff (DIS) concentrates on collecting intelligence related to weapons and military capabilities. Though an intelligence organization, it is not discussed in this chapter.

12. C. M. Andrew, *Secret Service: The Making of the British Intelligence Community* (London: Heinemann, 1985), p. 694.

13. See Christopher Andrew and David Dilks, eds., *The Missing Intelligence Dimension: Governments and Intelligence Communities in the Twentieth Century* (Urbana: University of Illinois Press, 1984), p. 10.

14. R. Jeffries-Jones, "The Role of British Intelligence in the Mythologies Underpinning the OSS and early CIA," *Intelligence and National Security* 15 (Autumn 2000).

15. An "illegal" was an intelligence officer based overseas who did not have official diplomatic cover for his activities. The term Great Illegals was used to designate a group of Soviet intelligence officers during the 1930s who were particularly successful at recruiting and running spies.

16. The Foreign Office is the British equivalent to the U.S. State Department. At this point, it was officially known as the Foreign and Colonial Office, but for simplicity's sake, it is fair to refer to it as the Foreign Office.

17. Fellow is the title given to a member of the faculty at a particular college at Cambridge University.

18. S. Rimington, *Open Secret,* 2nd ed. (London: Arrow, 2002).

19. C. M. Andrew, *Secret Service: The Making of the British Intelligence Community* (London: Heinemann, 1985), p. 696.

20. The use of the phrase "Honourable Members" is part of the language used in the House of Commons to refer to fellow Members of Parliament. The protocol is that the names of individuals are not to be used.

21. W. Wark, "In Never-Never Land? The British Archives on Intelligence," *Historical Journal* 35 (March 1992), pp. 195–202.

22. R. J. Aldrich, "Never-Never and Wonderland: British and American Policy on Intelligence Archives," *Contemporary Record* 8 (Summer 1994), pp. 132–50.

23. N. Moss, *Klaus Fuchs: The Man Who Stole the Atom Bomb* (New York: St. Martin's Press, 1987); R. C. Williams, *Klaus Fuchs, Atom Spy* (Cambridge, MA: Harvard University Press, 1987).

24. This American material was successful synthesized with existing material on the Cambridge spies in V. W. Newton, *Cambridge Spies: The Untold Story of Maclean, Philby and Burgess in America* (Lanham: Madison Books, 1991).

25. O. Tsarev and N. West, *The Crown Jewels* (London: Harpers & Collins, 1998); A. Weinstein and A. Vasiliev, *The Haunted Wood: Soviet Espionage in America—the Stalin Era* (New York: Random House, 1999).

26. A. Feklisov, *The Man Behind the Rosenbergs* (New York: Enigma Books, 2001); P. Sudoplatov, A. P. Sudoplatov, J. L. Schecter, and L. Schecter, *Special Tasks: The Memoirs of an Unwanted Witness* (London: Little, Brown, 1994); Y. Modin, *My Five Cambridge Friends* (London: Headline, 1994).

27. R. J. Aldrich, "Never-Never and Wonderland: British and American Policy on Intelligence Archives," *Contemporary Record* 8 (Summer 1994), pp.132–50.

28. Sir Stephen Lander, "British Intelligence in the Twentieth Century," *Intelligence and National Security* 17 (Summer 2002), pp. 7–20.

29. R. J. Aldrich, "'Grow Your Own': Cold War Intelligence and History Supermarkets," *Intelligence and National Security* 17 (Summer 2002), pp.135–51.

30. N. West, "Banned Books," in *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer,* ed. H. B. Peake and S. Halpern (Washington, DC: NIBC Press, 1994).

31. C. Cram, "Of Moles and Molehunters," *Studies in Intelligence* (October 1993), available at http://cicentre.com/Documents/DOC_Of_Moles_and_Molehunters.htm.

32. S. Rimington, *Open Secret*, 2nd ed. (London: Arrow, 2002).

33. R. J. Aldrich, "Never-Never and Wonderland: British and American Policy on Intelligence Archives," *Contemporary Record* 8 (Summer 1994), pp. 132–50.

34. C. M. Andrew and D. Dilks, eds., *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century* (Urbana: University of Illinois Press,

1984), p. 3. As an example of inaccurate and fantastical pre–World War I spy stories, they cited William Le Queux, a popular novelist whose accounts of cunning and ruthless German spies in Britain were best sellers. As a contemporary example, the authors cited the Thames Television "documentary" series, *Reilly: Ace of Spies*.

35. R. J. Aldrich, "Policing the Past: Official History, Secrecy and British Intelligence Since 1945," *English Historical Review* 119 (September 2004), pp. 922–64.

36. D. Reynolds, "The ULTRA Secret and Churchill's War Memoirs," *Intelligence and National Security* 20 (June 2005), pp. 209–24.

37. Ibid.

38. J. C. Masterman in the preface to his book *The Double Cross System*, published in 1972. Quoted in K. G. Robertson, *British and American Approaches to Intelligence* (Basingstoke: Macmillan, 1987), p. 262.

39. For further information on this, see R. L. Benson and M. Warner, eds., *VENONA: Soviet Espionage and the American Response*, *1939–1957* (Washington, DC: Central Intelligence Agency & National Security Agency, 1996).

40. F. H. Hinsley, et al., *British Intelligence in the Second World War. Volume 4: Security and Counter-intelligence* (London: Her Majesty's Stationary Office, 1990), p. ix.

41. T. Enever, *Britain's Best Kept Secret: ULTRA's Base at Bletchley Park* (Trowbridge: Bramley Books, 1999), pp. 10–12.

42. I am indebted to Professor Andrew for this point. He cites Martin Gilbert, Stephen Ambrose, and John Lewis Gaddis as prominent examples of this limitation. C. M. Andrew, "Intelligence in the Cold War: Lessons and Learning," in *Agents for Change: Intelligence Services in the 21st Century,* ed. H. Shukman (London: St. Ermin's Press, 2000), pp. 2–3.

43. David Kahn and Christopher Andrew are two notable exceptions.

44. C. Cram, "Of Moles and Molehunters," *Studies in Intelligence* (October 1993), at http://cicentre.com/Documents/DOC_Of_Moles_and_Molehunters.htm.

45. C. M. Andrew, "The British View of Security and Intelligence," in *Security and Intelligence in a Changing World,* ed, A. S. Farson, D. Stafford, and W. K. Wark (London: Frank Cass, 1991), pp. 10–24.

46. Pincher's book comes with the brilliantly melodramatic title, *Their Trade Is Treachery.*

47. Aberystwyth University offers a degree in intelligence studies, while courses at Cambridge, Nottingham, and King's College, London, among others, offer modules specializing in the study of intelligence.

48. R. J. Aldrich, *Espionage, Security and Intelligence in Britain*, 1945–1970 (Manchester: Manchester University Press, 1998).

49. C. M. Andrew, "Historical Attention Span Deficit Disorder: Why Intelligence Analysis Needs to Look Back Before Looking Forward," New Frontiers Conference, Rome, 2004.

50. D. Walker, "Just How Intelligent?" *Guardian*, February 18, 2003.

51. C. M. Andrew and V. Mitrokhin, *The Mitrokhin Archive: The KGB in Russia and the West* (London: Penguin, 2000); C. M. Andrew and O. Gordievsky, *KGB: The Inside Story of Its Foreign Operations From Lenin to Gorbachev,* 2nd ed. (London: London, 1991).

52. D. Walker, "Just How Intelligent?" *Guardian*, February 18, 2003.

53. For further details, readers can refer to the newly created SIS website, at http://www.sis.gov.uk. Those interested in intelligence careers can now apply online to become the next James Bond.

54. http://www.cia.gov/csi/index.html.

55. Dr. Rob Johnson, an American anthropologist, carried out fieldwork at the Central Intelligence Agency headquarters at Langley. He presented his findings to the Cambridge Seminar in the autumn of 2004.

BIBLIOGRAPHY

Aldrich, R. J. "Never-Never and Wonderland: British and American Policy on Intelligence Archives." *Contemporary Record* 8 (Summer 1994), pp. 132–50.

———. "Policing the Past: Official History, Secrecy and British Intelligence since 1945." *Canadian Association for Security and International Studies* (September 2002).

———. "'Grow Your Own': Cold War Intelligence and History Supermarkets." *Intelligence and National Security* 17 (Summer 2002), pp.135–51.

Andrew, C. M. *Secret Service: The Making of the British Intelligence Community.* London: Heinemann, 1985.

———. "Whitehall, Washington and the Intelligence Services," *International Affairs* (Royal Institute of International Affairs 1944–), 53, no. 3 (July 1977), pp. 390–404.

———. "The British View of Security and Intelligence." In *Security and Intelligence in a Changing World,* edited by A. S. Farson, D. Stafford, and W. K. Wark. London: Frank Cass, 1991.

———. "Historical Attention Span Deficit Disorder: Why Intelligence Analysis Needs to Look Back Before Looking Forward." New Frontiers Conference, Rome, 2004.

Andrew, C. M., and D. Dilks (eds.). *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century.* Urbana: University of Illinois Press, 1984.

Bennett, G. "Declassification and Release Policies of the UK's Intelligence Agencies." *Intelligence and National Security* 17 (Summer 2002), pp. 21–32.

Cram, C. "Of Moles and Molehunters." *Studies in Intelligence*. October 1993 Accessible at http://www.cia.gov/csi/kent_csi/Default.htm.

Hinsley, F. H., and C. A. G. Simkins. *British Intelligence in the Second World War. Vol. IV: Security and Counter-intelligence.* London: Her Majesty's Stationery Office, 1990.

Jeffries-Jones, R. "The Role of British Intelligence in the Mythologies Underpinning the OSS and Early CIA." *Intelligence and National Security* 15 (Autumn 2000), pp. 5–19.

Lamphere, R. L., and T. Schachtman. *The FBI and KGB War.* New York: Random House, 1986.

Lander, Sir Stephen. "British Intelligence in the Twentieth Century." *Intelligence and National Security* 17 (Summer 2002), pp. 7–20.

Reynolds, D. "The ULTRA Secret and Churchill's War Memoirs." *Intelligence and National Security* 20 (June 2005) pp. 209–24.

Rimington, S. *Open Secret,* 2nd ed. London: Arrow, 2002.

Robertson, K. G. *British and American Approaches to Intelligence.* Basingstoke: Macmillan, 1987.

Walker, D. "Just How Intelligent?" *Guardian*. February 18, 2003.

Wark, W. "In Never-Never Land? The British Archives on Intelligence." *Historical Journal* 35 (March 1992), pp. 196–203.

West, N. "Banned Books." In *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer,* edited by H. B. Peake and S. Halpern. Washington, DC: NIBC Press, 1994.

Wright, P. *Spycatcher.* Richmond, Victoria, BC: William Heinemann, 1987.

4

DEMOCRATIC DEFICIT BE DAMNED

The Executive Use of Legislators to Scrutinize National Security in Canada

STUART FARSON AND REG WHITAKER

INTRODUCTION

HISTORICALLY, CANADA HAS LOOKED IN TWO DIRECTIONS when developing governance systems. Unsurprisingly, as a former British colony, many British ideas remain firmly embedded. Such crucial notions as responsible government, a constitutional monarchy, the type of Parliament, a nonpartisan public service, as well as its common law legal system are all derived from the British experience. But from its earliest days, Canada also drew on concepts developed by its southern neighbor, the United States of America. From there stems its federal system, a written constitution with protected liberties, the idea of judicial review, access to information legislation and, more recently, sunset clauses and statutory protections for whistle-blowers.

In one area Canada has demonstrated a particular reluctance to follow its neighbor's lead—the oversight of intelligence. During the 1970s Canada and the United States undertook comprehensive inquiries into their intelligence communities. In the United States, newspaper articles by Seymour Hersh sparked that development. A presidential commission was first off the blocks, followed by two special congressional committees. Of these, the one chaired by Frank Church in the Senate proved the more influential. Important reforms resulted at all levels of government. The president appointed two new advisory boards—one concerning oversight specifically, the other intelligence more broadly. Administratively, the Inspector General's role was expanded to cover most government departments, including intelligence agencies. Finally, Congress entrenched new Select Committees on Intelligence in both of its houses with full purview over all intelligence organizations, save the Federal Bureau of Investigation.

In Canada, John Sawatsky's newspaper articles encouraged the Québec government to appoint an inquiry into the activities of the Royal Canadian Mounted Police (RCMP)'s Security Service in that province. This forced the federal government to establish its own public inquiry under Justice David McDonald. Though the McDonald Commission recommended a complementary system of independent scrutiny by arms-length review bodies and monitoring by a new permanent committee of Parliament covering all intelligence organizations, the government envisaged legislation of lesser scope. It provided only internal and external review bodies to cover the newly formed Canadian Security Intelligence Service (CSIS), which replaced the now-disbanded Security Service. With the external review body, the Security Intelligence Review Committee (SIRC), being posited as Parliament's "surrogate," the legislature's role was limited to reviewing the enabling legislation five years after enactment without any relationship being defined that would permit easy transfer of information between the two.

Matters have remained largely the same in both countries ever since. In Canada, there were repeated calls for a permanent parliamentary committee. But these fell on deaf bureaucratic ears, with only the occasional former official rising to rebut "alien" American oversight ideas.[1] In two respects, however, greater scrutiny was achieved. The Auditor General, a parliamentary servant, previously mum on the subject of intelligence, became more vocal, providing a series of insightful reports on the capacities of Canadian intelligence. Also in the 1990s, the Communications Security Establishment (CSE), Canada's signals intelligence agency, was finally brought under an albeit limited form of review. This was achieved in an unusual way. A motion on the parliamentary Order Paper garnered all-party support for establishing a Commissioner for the CSE, which led the government to establish that office. The commissioner was, however, only charged with ensuring the agency's compliance with Canadian law.[2] There was neither any mandate to consider its capacity or performance, nor one to identify whether the extant law was adequate, arguably crucially important for any rapidly changing technological field.

More recently the former Liberal government and the new Conservative government have shown interest in increasing scrutiny of Canada's intelligence community and broadening Parliament's involvement in judicial appointments, both mechanisms for addressing the "democratic deficit." Close observers of the committee processes chosen to consider these changes would have noted that their deliberations were often replete with irony and that their outcomes were potentially paradoxical. In early 2004, the Liberal government asked a permanent standing committee of Parliament to consider how Parliament might best be involved in judicial appointments. At the same time, it asked an interim committee of parliamentarians to consider how best to involve Parliament in scrutinizing the secret world. In the first instance, the standing committee recommended an ad hoc committee of parliamentarians, a process that was duly followed by the new Conservative government before the new session of Parliament was officially

opened. In the second case, the ad hoc committee of parliamentarians advocated that a permanent committee of Parliament provide the scrutiny, a decision subsequently ignored by the Liberal government. One might well ask: How could two committees—sharing the same chair—develop such contradictory positions? This chapter is concerned with attempting to square this circle. An initial suggestion is that it can, if three variables are carefully considered: whether the "democratic deficit" is redressed in the process; whether the institutions needing scrutiny deserve special treatment; and finally, whether there are any historical precedents that bear on the outcomes.

To take the two last points first, unlike the British Parliament, which until recently had law lords debating in the upper chamber, the Canadian Parliament has studiously avoided direct contact with members of the judiciary in any official parliamentary setting. Underpinning this was a perceived need to avoid any precedent that might limit Parliament's prerogatives or its members' privileges. Thus, when Parliament reviewed the Canadian Security Intelligence Service Act in 1989–90, the MPs involved did not meet with the specially designated judges of the federal court who heard CSIS's warrant applications. It sent senior staff to meet informally with the court's administrator. It also suggests Parliament's reluctance to require the first commissioner of the CSE, a former appellate court justice, to appear before them on his annual reports. Thus, by viewing things through this lens, recommending that an ad hoc committee of parliamentarians—not a standing committee—review Supreme Court appointments exhibits consistency, not difference.

However, the decision not to adopt the Interim Committee's recommendation that a permanent standing committee of Parliament should scrutinize Canada's intelligence community has much to do with historical precedent. Canada is one of the few countries to have had one of its members of Parliament (MPs) successfully prosecuted on espionage charges. Though this happened shortly after World War II, it has contributed to an enduring deep bureaucratic mistrust of MPs as far as any involvement in the secret world goes. They are thus frequently described—at least when Chatham House rules apply—as not being trustworthy, having a propensity to place their own political interests ahead of national ones. Unfortunately, some evidence supports this position. The hearings into how Mr. Al-Mashat, the former Iraqi Ambassador to the United States, gained rapid landed immigrant status to Canada were among the most politically charged in recent memory. Few can forget the unseemliness of bureaucrats, many of them senior diplomats, being forced for political reasons to expose their personal as well as professional differences. Yet, it must be said, such examples are much fewer and farther between than some would have us believe. The examples where parliamentary committees work very collegially, of course, do not garner headlines. In this regard it should be noted that the special committee that reviewed the CSIS Act and Security Offences Act was such a committee. On only one issue during its year of existence was a vote called. What follows addresses the first variable: whether the measures advocated truly offered redress for democratic deficit.

THE IMPACT OF THE TERRORIST ATTACKS ON WASHINGTON AND NEW YORK

Besides instigating new omnibus legislation—the U.S. Patriot Act—and needed security and intelligence reforms, the terrorist attacks on New York and Washington of September 2001 revived interest in oversight. The formation of the new Department of Homeland Security (DHS), in fact, constituted the biggest governmental restructuring since World War II. Several inquiries—some congressional, some appointed by the president—recommended sweeping changes to security and intelligence structures, and congressional oversight. Of particular importance in the latter regard were the numerous committees and subcommittees that had responsibility for the DHS's budget.

Following the attacks, the Liberal government of former Prime Minister Jean Chrétien also quickly tabled the Anti-Terrorism Act and provided new funds to enhance security and intelligence. Though similar in many ways to the U.S. Patriot Act, the legislation incorporated elements long on the intelligence bureaucracy's wish list. Because of its omnibus nature many components did not receive the scrutiny they deserved. Substantive change, however, to Canada's security and intelligence community would have to wait until the prime minister's retirement.[3]

THE "DEMOCRATIC DEFICIT" AND NATIONAL SECURITY REFORM

On becoming leader in December 2003, Paul Martin immediately placed his stamp on the new administration. His first order of business was to attend to what he termed the "democratic deficit." Canada's Parliament was not performing the role that either the Canadian public or its elected representatives believed it should.[4] To redress the balance, two things were necessary. Parliament had to be restored to the center of the decision-making process, and the capacity of parliamentarians to shape national policy needed enhancement. The new administration's core principles were now "transparency, accountability, financial responsibility, and ethical conduct."[5] Martin promised several new initiatives to reflect this priority. Among them was a commitment to revamp the committee process through additional resources for research and support services. However, none of these initiatives were realized.

In assessing the quick demise of these democratic deficit initiatives, the damaging political context that engulfed the Martin government must be specified. Although at the time of his accession to the highest office Mr. Martin was widely believed likely to win a fourth consecutive Liberal majority government when he went to the polls, the future of his government was immediately threatened when the auditor general (an officer of Parliament) revealed a serious

financial scandal implicating the former Chrétien government—in which Mr. Martin had been the most prominent minister—in widespread abuse of public funds. Seeking to deflect the so-called sponsorship scandal onto his predecessor's shoulders, the new prime minister, denying any personal knowledge of wrongdoing, called a public inquiry into the affair. This only served to provide sensational testimony damaging to the Liberal Party's public image, while splitting the party between Chrétien and Martin loyalists. In the 2004 election, the Liberals limped to a fragile minority, were defeated in the House in late 2005, and lost to their Conservative rivals in the winter election of 2006. Even prior to the 2004 election, the opposition parties, smelling blood, were in no mood to give any consideration to the democratic deficit proposals to revamp Parliament. With the Martin minority of 2004–5, Parliament became a brutally partisan place where sheer survival was the goal of the government, and precipitating an early election was the goal of most of the opposition parties. In this poisonous atmosphere, it is difficult even in retrospect to lay partisan blame for the ignominious decline of the democratic deficit issue: Neither government nor opposition had any interest in reforming Parliament to expand democracy when partisan life or death was the real issue.

The ill-fated Martin government had rather more success with its administrative revamping of national security policy and practice within the federal government. A major priority for the new government concerned a series of far-ranging initiatives aimed at securing Canada's public health and safety. Of critical importance was the establishment of a new Department of Public Safety and Emergency Preparedness Canada (PSEPC). This portfolio would be headed by the Deputy Prime Minister. It included the agencies of the old Solicitor General's department, and a new Border Services Agency, which integrated the investigative arms of the Department of Citizenship and Immigration, Customs, and the Food Inspection Agency. In addition, the Office of Critical Infrastructure and Emergency Preparedness, which had hitherto been culturally adrift in the Department of National Defence, was brought under the PSEPC umbrella. In many respects PSEPC reflected the DHS's formation. However, it differed in two important respects. The Department was focussed around CSIS, the agency primarily responsible for gathering security intelligence, and the RCMP, the federal police force, also with significant intelligence capacities. Other important developments included: the creation of a new Cabinet Committee on Security, Public Health and Emergencies, with special responsibilities for managing national security and intelligence matters and for coordinating the response to emergencies; a new position of National Security Advisor to the Prime Minister in the Privy Council Office who would be responsible for intelligence and threat assessment as well as helping the Minister of PSEPC in the development of national security and emergencies policy; and a new public health agency to address public health risks and to coordinate national responses to health crises.

DEMOCRATIC DEFICIT: IMPROVED OR BE DAMNED?

On one important matter the prime minister lodged only a "proposal," as it technically lay within Parliament's prerogative. This concerned the establishment of "a National Security Standing Committee in the House of Commons." Here he made a commitment to make its members Privy Councillors so that they could be fully briefed on national security issues.[6] However, over the course of the parliamentary recess, which continued from late December 2003 until early February 2004, this proposal was changed significantly. When the Government tabled its Action Plan for Democratic Reform on February 4, 2004, in the Commons, it stated only that it would consult with parliamentarians on the creation of a "National Security Committee of Parliamentarians."

To those unfamiliar with Parliament's working, this subtle change of wording may not seem significant. But it is crucially important to Parliament in its ability to hold the Executive to account and to define the breadth of purview for scrutinizing government actions. With a quick stroke of a pen one had moved from a committee situated within the House of Commons, with all the powers and privileges of Parliament fully entrenched under the constitution, to an executive instrument that the administrative arm of government could appoint and firmly control. Instead of having robust powers of scrutiny like Congress's Select Committees on Intelligence, the government now proposed something similar to the British model, a body with the appearance of being parliamentary through its membership, but that had, in fact, little to do with Parliament, and that would have limited access, few resources, and little control over the selection and appointment of staff. Clearly, as afficionados of the British political satire *Yes Minister* recognized, the spirit of Sir Humphrey Appleby had visited Ottawa over the parliamentary recess just in time to convince the powers that be to change their minds in favor of a "safer administrative option," one that would do nothing to offset the democratic deficit, only increase it.[7] The entrenched bureaucratic distrust of MPs and their perceived proclivity for pursuing personal political objectives ahead of the national interest had won the day.

THINKING INSIDE THE REVIEW-OVERSIGHT BOX

Further evidence of this lexiconic sleight of hand was provided when the deputy prime minister tabled a consultation paper on the National Security Committee of Parliamentarians in the House of Commons on March 31, 2004. This paper was not prepared by the Privy Council Office, as one might reasonably have expected, but by an outside consultant. His terms of reference were not to consider matters relating to the National Security Standing Committee of the House of Commons, which the Prime Minister had, in fact, originally announced. Instead, they were to explore "options pertaining to the creation of a National Security

Committee of Parliamentarians *as announced by the Prime Minister on December 12, 2003*."[8] The intent of the paper was to inform decisions on the proposed status, mandate, and structure of the new committee, with a view to formulating recommendations by fall 2004.[9] Apparently, the purpose of the committee was now only "to ensure that parliament was more informed on national security issues, leading to better decision making from which all Canadians stood to benefit."[10] No mention was made of the need for better accountability, perhaps the quintessential function of Parliament, or measures to reduce the democratic deficit, or even how the public's lack of trust in parliamentarians might be addressed.

THE GOVERNMENT'S CONSULTATION PAPER: THEMES AND STRUCTURE

The introductory section of the paper[11] covered two main themes. The first was the wider context of democratic reform in which the committee would be situated. Here emphasis was placed on an enhanced role for parliamentarians and parliamentary committees "to shape laws and hold the Government to greater account."[12] The second concerned the existing security environment. It posited that the current threat of "global terror" would continue to consume public attention and resources for the foreseeable future. It was the government's view that, under these circumstances, it was desirable to have a "body of informed parliamentarians from whom to seek advice" and that any review of national security issues should be pursued in a non-partisan manner.[13] The section also drew attention to the distinction between "sensitive information" and "classified information." In particular, it noted that sensitive information "(was) a wider class of information whose disclosure to the public would be injurious to international relations or national defence or national security and which is therefore classified."[14]

Three further matters were raised. The first was the old argument concerning the meaning of "oversight" and "review." The former was defined only in terms of its supposed U.S. context as "supervision," and was said to imply the management and direction of particular bodies in ways that would blur accountability because of a shared responsibility between the executive and legislative branches of government. It suggested that the oversight function in Westminster systems of government was the responsibility of ministers alone. Review was seen only in after-the-fact terms. Nevertheless, it was viewed as an important and necessary element of accountability in Westminster systems because it provided an independent assessment of past performance.[15]

The difference between two key constitutional conventions—responsible government and the separation of powers—in the Westminster and congressional systems of government were touched upon only very briefly. In the case of responsible government, the paper drew a distinction between those things for which a minister is directly responsible and those that are administered by independent

agencies operating at arm's length from the minister. In this context, independent bodies like SIRC, which reviews the actions of the CSIS and the Commissioner for the Communication Security Establishment, whose office reviews Canada's equivalent of the National Security Agency, were said to have mandates that "(had) a significant bearing on the character of Parliamentary review."[16]

Finally, the section drew attention to the RCMP's national security duties. Here it acknowledged that the existing independent body charged with reviewing the Force's activities—the Commission for Public Complaints against the RCMP—appeared to be inadequate for national security investigations. In this regard it noted the new government's commitment to establish an independent arm's-length review mechanism for such investigations on coming into office and that Justice Dennis O'Connor had been asked for proposals as part of his public inquiry into matters relating to the Maher Arar affair.[17]

The section titled "Past and Current Practices" began by providing a brief history of Parliament's interest in and review of Canada's security and intelligence community. Here it noted that when CSIS was established in 1984, the government of the day suggested that, by referring SIRC's annual report to the appropriate Standing Committee, Parliament would "have both the opportunity and responsibility to review the report and assess the activities of CSIS."[18] There was also a brief description of current parliamentary practices and the committees that have scrutinized Canada's security and intelligence community. There was, however, no substantive discussion of the powers of Parliament, the objectives and remits of the relevant committees, or any previously shortfalls in its capacity to scrutinize intelligence that Parliament had identified. The paper asserted that there was a duplication of effort between the Senate and the House of Commons and that the two bodies provided different advice without any assessment of their different contributions or explanations about why this might occur.[19] It noted that there were three independent review bodies that operated at arm's length from ministers and reported to Parliament.

In Part II the consultation paper turned its attention to practices elsewhere. Only matters in Australia, Britain, New Zealand, and the United States were considered. The only rationale for this appears to be that these states represent Canada's closest and longest serving intelligence partners. In the case of Australia the paper correctly identified the key agencies and review bodies. But it did not explain why Australia decided in 2001 to change parliamentary modes and methods of scrutiny. In the case of the United Kingdom, the paper suggested that "parliamentary review" was introduced in 1994 with the adoption of the Intelligence Services Act. In fact, the Intelligence Services Committee was not a committee of Parliament but a committee of parliamentarians. In suggesting such a thing the paper glosses over the work of select committees, particularly those dealing with Home and Foreign Affairs. It also conveniently omitted any discussion of the reasons why its chief investigator had been fired and by whom. In none of the Westminster systems identified was there any discussion of the powers of their parliaments, the resources available, or how police involvement

in national security matters were reviewed. Part II was also at pains to stress how different the congressional system was from the Westminster model. At one point it suggested that "Congress does not review the actions of security and intelligence agencies, it has *oversight* of them."[20] It did so without any substantive analysis of how the two functions really differ.

The final part of the consultation paper dealt with issues related to the status, mandate, and procedures of a national security committee. In trying to settle these, it focused on the last two first in the hope that parliamentarians would conclude that a committee of parliamentarians was the best option. The consultation paper saw "the overarching purpose of parliamentary review (being) to improve the effectiveness of (Canada's) security arrangements by making them more accountable *through the central organ of democracy, the Parliament of Canada*."[21] It believed such a mandate was best achieved by a general review of the overall performance of security agencies. Furthermore, it appeared against the idea that a parliamentary committee should review the reports of review bodies or those of the security agencies, and favored setting strict limits on what Parliament could see. Parliament ought to focus only on large strategic issues and matters of policy rather than operations.

The final part also considered the membership of the committee, how individuals would be selected, the size of the committee, the tenure that politicians should have, what information they should see, whether they should be security cleared, the staff they should have, and whether that staff should come from the Privy Council Office or from Parliament. Also considered were the location of meetings and whether they should be closed-door or in public, and whether reports should be vetted before being released for public consumption.

The final issue concerned the status of the committee and what form it should follow. Here only three models were discussed: a Joint Committee of the House of Commons and Senate, established under existing standing orders; a legislated committee reporting to the House and Senate, as if it were established under existing standing orders; and a legislated committee reporting to the prime minister, with the requirement that its reports be tabled in Parliament. Of these, it firmly favored some form of legislated committee. The rationale for this seemed to be that because the Australian, British, and New Zealand models were legislated, so too should the Canadian model.

A CRITICAL ASSESSMENT OF THE CONSULTATION PAPER

Perhaps the most important criticism that can be levied against the consultation paper is that it does not appear to be informed by any analysis of Parliament's past difficulties in scrutinizing intelligence. Nor is there any indication that it is cognizant of the now-vast academic literature on the subject. This is in stark contrast to the consultation paper prepared for the Maher Arar inquiry.[22]

This was clearly based on research papers provided by leading academics in the field of intelligence, security, and antiterrorism legislation.[23]

This deficiency has important ramifications in a number of different ways. Perhaps the most important of these is that it leaves the consultation paper without any strong theoretical underpinning other than a reliance on the old and often abused argument that there is a constitutional distinction to be drawn between review and oversight. The extant literature argues that effective scrutiny of security and intelligence bodies depends on legislative bodies doing much more than after-the-fact reviews.

CONGRESSIONAL OVERSIGHT AS A PARLIAMENTARY MODEL?

Though "oversight" was a term infrequently used outside the United States until the early 1990s, it is now widely employed to imply a comprehensive approach to scrutinizing, not supervising, the actions and inactions of government of a variety of democratic stripes. More significant, it is readily used in this manner in the parliamentary context.[24] Important contributors to this debate have been Peter Gill,[25] Laurence Lustgarten, and Ian Leigh,[26] and, more recently, the extensive comparative work of the numerous contributors to the various projects on this and related subjects by the Geneva Centre for Control of the Armed Forces, particularly that prepared in conjunction with the Inter-Parliamentary Union.[27] All have attempted to develop theoretical frameworks for the oversight and accountability of security and intelligence agencies. Furthermore, it should be noted that official government websites in Australia and the United Kingdom now readily use the term.[28]

Dismissing congressional oversight purely on the grounds that it is not appropriate for parliamentary democracies because it blurs lines of responsibility and hence accountability is subject to challenge. Though some authorities agree that there is an element of supervision in the oversight process, they also suggest that the term "oversight" has a much broader connotation and also implies review and monitoring of government action.[29] Both may better be understood as scrutiny of government, and as a necessary element of the legislative process. Experts also note that oversight takes place in a number of venues—but especially in committees—and has a number of overlapping objectives and purposes. Frederick Kaiser, a long-standing employee of the Congressional Research Service, for example, suggests that congressional oversight serves to:

- Improve the efficiency, economy and effectiveness of government operations;
- evaluate program performance;
- detect and prevent poor administration, waste abuse, arbitrary and capricious behaviour, or illegal and unconstitutional contact;

- protect civil liberties and constitutional rights;
- inform the general public and ensure that executive policies reflect the public interest;
- gather information to develop new legislative proposals or to amend existing statutes;
- ensure administrative compliance with legislative intent; and
- prevent executive encroachment on legislative authority and prerogatives.[30]

Though it might be possible from a Westminister perspective to quibble with "prevent[ing] poor administration" and "ensur[ing] administrative compliance with legislative intent," these points are generally unexceptionable in terms of parliamentary democracy.

The American literature is also important in several ways. Not only does it stress that oversight has its limitations and weaknesses, but it indicates that it is steadily changing and evolving.[31] Some of the literature is particularly useful in showing how different forms of oversight are needed to achieve different objectives. For example, Paul Light has shown that different forms of accountability require different forms of scrutiny. Evaluating capacity requires before-the-fact scrutiny. Compliance auditing is best done after the fact. Developing performance benchmarks, however, requires both before- and after-the-fact forms of scrutiny.[32]

Other research suggests why members of Congress decide to scrutinize particular aspects of government and not others at particular moments in time. Initially, the dominant view of congressional oversight was that it intruded inappropriately on the executive function. Subsequently, congressional oversight was criticized by Bibby and other Republicans in the late 1960s as being neither comprehensive nor systematic.[33] As a result, many people complained that Congress had "neglected" its oversight role and had lost control over the executive branch in the process. Such views were challenged initially on theoretical and later empirical grounds. In the 1970s, Ogul noted that one's view of sufficiency depended on how one defined oversight, the policy preferences one held, and the models of legislative behavior to which one adhered. In short, students of legislative oversight were "like most people, prisoners of the pictures in their heads."[34]

Building on the work of Ogul, Mathew McCubbins and Thomas Schwartz directly challenged the insufficiency view in the early 1980s.[35] They argued that Congress had not neglected its oversight role. Instead, it had for political reasons tended to choose a "fire-alarm" approach over a "police-patrol" mode of oversight. The fundamental difference between the two is that in the police-patrol model Congress is proactive, which is to say it first has to troll for potential problems. By contrast, in the fire-alarm approach Congress is essentially reactive, responding to outside influences and complaints. McCubbins and Schwartz built their challenge on three assumptions. One of these, the motivational assumption, talks directly to the issue of oversight effectiveness. They see members of Congress as politicians rather than statesmen. This implies adopting methods that

produce the best political results for themselves. This, in turn, means avoiding strategies that might incur blame and taking those that permit the greatest amount of credit to be gleaned. As a result, members of Congress avoid police-patrol forms of oversight because such analyses can produce evaluations that do not reveal serious problems that need fixing. Instead, they maximize their time in two particular ways. First, they choose to scrutinize situations where a potential problem has already been revealed and where likely supporters have shown concern. Second, they limit the overall time spent on oversight so that they can devote themselves to other pressing matters. In doing this, however, members of Congress frequently do not use an all-or-nothing approach. They use one that is predominantly of the fire-alarm mode. Further, it should be stressed that McCubbins and Schwartz do not contend that a fire-alarm approach is either more effective than the police-patrol model or more likely to serve the public interest. Rather, they suggest it is more likely "to secure greater compliance with legislative goals; whether such compliance serves the public interest depends on what those goals are."[36] Their greater efficacy argument is based on two points. First, legislative goals are seldom stated precisely, making it difficult to decide when inappropriate action has occurred. As a result, using complaints as a starting point permits Congress to give greater clarity to legislative intent. Second, a police-patrol approach likely misses many such opportunities because it would only sample executive branch actions. Significantly, McCubbins and Schwartz make the following broader claim:

> Although our model refers only to Congress, we hazard to hypothesize that as most organizations grow and mature, their top policy makers adopt methods of control that are comparatively decentralized and incentive based. Such methods, we believe, will work more efficiently (relative to accepted policy goals) than direct, centralized surveillance. This is sufficiently plausible that we wonder why students of Congress have generally assumed that congressional oversight must be of the direct, centralized police-patrol variety. Part of the reason, perhaps, is that Congress itself applies the label "oversight" to subcommittees charged with police-patrol responsibilities.[37]

Such an analysis focused attention on the meaning of oversight, particularly on the difference between what it implied in theory and in practice. The law clearly depicted Congress's duty as a very comprehensive one that most careful analysts recognized as an impossible task. By contrast, studies of practice depicted it as a highly selective process. Thus, Ogul's earlier warning took on renewed meaning. In the mid-1970s, he had posited correctly that one's assessment of oversight was directly related to how it was defined:

> If oversight is defined only in terms of formal powers, different conclusions emerge about its adequacy than if informal relations are taken into account. Those who view oversight as simply an attempt to influence the implementation of legislation through post statutory investigations will reach different conclusions than those who are sensitive to oversight performed latently.

> How oversight is defined affects what oversight one finds. Writers assess oversight differently at times because they are not talking about the same thing. These differences are also mirrored in vocabulary. Thus the words scrutiny, review, inspection, control, command, supervision, watchfulness, and influence each carry connotations about what is expected. The Joint Committee on the Organization of Congress worried at some length about appropriate terminology to describe the oversight function. Part of this groping reflected competing conceptions of reality. *Their choice of "review" to replace "oversight" clarified very little.*[38]

According to Keefe and Ogul, politics largely explains why oversight is partial, selective, and reflective of legislators' choices. Those involved are normally confronted by competing priorities and time pressures. Frequently, they lack the expertise to do the job properly and see little political payoff in the enterprise. The choices manifest themselves particularly in the techniques of control, the frequency and degree of perseverance applied, and who is involved. They are frequently affected by such matters as committees' structures, the personalities of the members, and the political events of the day.[39]

More recently, Aberbach has noted an increase in both the level of formal oversight, particularly regarding the use of hearings, and the degree to which Congress pursues information about policy and administration. He has argued that this is primarily the result of a rise in the political rewards from oversight relative to other activities.[40] In addition, Aberbach has challenged McCubbins and Schwartz's thesis by asserting that the police-patrol, or proactive, approach is now the dominant mode of oversight practiced by Congress. He has rationalized this development on four points. First, a proactive approach is now more productive in the sense that greater benefits currently accrue per unit of time spent by congressional personnel. Second, the costs involved are now perceived to be less than before. Third, members of Congress tend to respond to such changes to their political and institutional environment. Finally, congressional resources, information networks, and expertise have changed significantly.[41] The result is that the bureaucracy is no longer in the overpowering position once foretold by Weber. Congress now has a "formidable counterorganization," its staff having both substantial expertise and well-developed information networks in their respective oversight areas. Such a rationalization offers a possible explanation for the supposed decline in oversight. Aberbach's evidence has suggested that it is not oversight overall that has declined but rather that following the fire-alarm approach.[42]

PARLIAMENT'S UNDERUTILIZED CAPACITY TO SCRUTINIZE GOVERNMENT

Another important criticism that may be levied against the consultation paper lies in its orientation. Not surprisingly, it looks at the world through the eyes of the executive branch. Thus, there is an emphasis on notions of responsible government and ministerial responsibility, not on Parliament's roles or powers. Besides

being situated as the place to debate the major affairs of the day and to adopt legislation, Parliament has important roles to play in both scrutinizing government action and holding ministers individually and collectively to account for them. Arguably, it is the job of Parliament as a whole to effect this, not opposition party members alone. Of course, to burden government members in this way is to place them in an awkward and potentially schizophrenic position.

This does indicate an important difference between parliamentary and congressional forms. In the latter, party discipline in the legislative branch is not required to maintain the executive, elected to a fixed term, in office. In parliamentary systems, on the other hand, governments stand or fall on the confidence of the House. This is an especially acute problem during periods of minority government, as has been the case in Canada since 2004. Members of Parliament, especially those on the government benches, thus face conflicting roles as partisans and parliamentarians. Yet this should not be seen as a bar to effecting parliamentary scrutiny of government, to the extent that such scrutiny falls short of actually raising the question of confidence, as such. In fact, scrutiny of government in committee does not raise confidence, which can only be brought by motion in the House as a whole, or by defeat of a major government bill involving the expenditure of public monies.

To effect greater scrutiny Parliament already has a strong arsenal of powers. The Standing Orders of the House of Commons, for example, provide Parliament *as a whole* with the authority to call for "people, papers and records."[43] To enforce this authority Parliament has the powers of subpoena and the capacity to hold people in contempt should they not provide the necessary materials. Parliament also has another important tool that it can bring to bear. Where a government department is not sufficiently forthcoming, it can vote, and has voted, to reduce that department's estimates. Although it is true that these powers are seldom used, the mere threat of their use has often proven sufficient to cause even the worst of recalcitrants to step into line.

The consultation paper does not really envisage what positive effects might result from truly effective scrutiny. In this regard it is appropriate to recall what a former Director of Central Intelligence told the Special Committee responsible for reviewing the CSIS Act and Security Offences Act when it visited Washington in 1990. When asked how he felt about congressional oversight by the intelligence committees, he responded as follows: "When it first came in we fought it all the way . . . Now we wouldn't do without it. When the media misrepresents our actions, we now have someone to call who can address the matter. When the Executive Branch fails to provide us with adequate resources, we have someone to go to bat for us."[44] Today, CSIS looks on its watchdog committee, SIRC, in much the same way, despite early rocky relations with its review body. When the Commissioner of the RCMP spoke in 2005 at the public hearings of the O'Connor inquiry into the Maher Arar affair, he went out of his way to welcome the idea of a stronger review mechanism to oversee the RCMP's national security law enforcement activities.

What this shifting sentiment clearly suggests is that legislative oversight is a two-way street. By making intelligence committees privy to the secret affairs of intelligence agencies, they can provide important benefits to the agencies concerned.

There is an implicit assumption in the consultation paper that both the internal review bodies and the external, independent, arm's-length review bodies are working as Parliament first envisaged or as effective oversight would demand. There is considerable evidence that this is not the case. Two Inspectors General of CSIS had trouble with the agency they were supposed to certify. In one case the inspector general was denied access to papers she thought she should have. In the other, the director of CSIS refused to meet with the inspector general for more than a year. When SIRC came into being, its reports had a certain edge to them. Today the relationship between the agency and the review body appears to be much more comfortable, which may be cause for concern. In 1989–90, the special committee that reviewed the CSIS Act was able—despite the road blocks put in its way—to establish that SIRC's research methods fell far short of what was desirable. Without a parliamentary committee having access to their files and reports, there is no way of knowing whether they remain so today. When the Anti-Terrorism Act was passed in late 2001, it included enhanced legal powers for the CSE. Arguably, the need for this new intrusive power might have come to light if the independent review body for the CSE had previously been mandated to consider the adequacy of existing law, not just compliance with it. It should also be noted that the first commissioner of the CSE declined Parliament's invitations to appear before the Sub-Committee on National Security. Given that his reports were of little substantive value to Parliament as mechanisms of accountability, this was of particular significance. He was also reticent to give public interviews even to bona fide researchers.

The consultation paper does not consider the Canadian literature that has examined Parliament's current capacity to hold ministers responsible for security and intelligence matters. When Parliament was obliged to conduct its five-year review of the "provisions and operation" of the CSIS Act and Security Offences Act, it was prevented from completing its mandate because it could not see such necessary documents as SIRC's reports, the inspector general's certificates, ministerial directives, and the Director of CSIS's Annual Report. Furthermore, Parliament found that SIRC, which had been positioned as its surrogate when the legislation was initially passed in 1984, would not speak openly to the committee even in closed-door sessions. Its members contested with good reason that they were prevented from doing so because of their oath of office.[45] Arguably, this situation should have been rectified before Parliament was obliged to establish a similar review committee in December 2004 to conduct a three-year review of the Anti-Terrorism Act. Whereas the CSIS Act was adopted and reviewed during a period of calm, the adoption the Anti-Terrorism Act was not. As a result, matters were enacted without the usual scrutiny that would normally have been imposed. For example, two pieces of legislation that had long been advocated but

were unlikely to get a smooth parliamentary passage—enabling legislation for the CSE and a revamped Official Secrets Act—were included in the package and were largely ignored during Parliament's consideration.

Perhaps not surprisingly the consultation paper is structured along organizational lines, not functional ones. Thus, again, lines of accountability focus on the responsibility of individual ministers for particular agencies. Here the emphasis is on intelligence collection agencies, not the mechanisms analyzing and assessing what is collected. This means that there is no real analysis of whether the extant review mechanisms are adequate or whether there are holes in the regime. Oversight and review are not likely to be effective for at least two reasons if they focus on single organizations when security and intelligence matters are considered. First, security and intelligence policy and operations tend to be cross-departmental functions of government. And since 9/11 they frequently involve both federal and regional institutions. Second, it is frequently the case that more than one agency is involved in a particular practice. This means that focus on single organizations is not likely to be particularly helpful when it comes to monitoring for compliance or establishing capacity and performance effectiveness. Although at the time of writing the O'Connor report has not yet been made public, it is already certain that O'Connor will recommend some form of more integrated external review to cover the increasingly integrated nature of security and intelligence operations, horizontally within government, and vertically between levels of government and between government and the private sector.

Finally, the consultation paper considered neither the likely impact that the 9/11 attacks would have on oversight needs nor the implications for Canada of its most important allies being unable to find weapons of mass destruction in Iraq that their intelligence assessments firmly posited were there. To take the second point first, it may be hypothesized that there is now a much greater need to consider whether Canada's intelligence analysis units are getting it right and are properly interpreting the intelligence they receive from their friends and allies. As well, the attacks have put pressure on the Canadian government to adopt preventive and investigative measures that run contrary to the beliefs of many Canadians concerning human rights and civil liberties. The threat of nuclear terrorism—if perceived to be substantive—will likely only exacerbate this situation. Under the circumstances a robust system of scrutiny that encourages both the effectiveness of intelligence and security organizations and the protection of human rights and civil liberties is in order. To achieve this, thinking outside traditional boxes is needed.

THE APPOINTMENT OF AN INTERIM COMMITTEE OF PARLIAMENTARIANS AND OTHER IRONIES

The government's decision in May 2004 to hold a June election had specific consequences for any detailed consideration of the consultation paper over the

summer months as the consequential dissolution stopped all work in Parliament. The question, however, of whether there should be a permanent standing committee of Parliament or merely a committee of parliamentarians was an issue on which Parliament had previously expressed an opinion and had a natural and distinct interest. It should, therefore, have been for Parliament to consider at the appropriate time in a manner of its choosing. Prime Minister Martin's initial "proposal" clearly respected this position.

The decision taken by the government concerning how to proceed with a parliamentary assessment of the consultation paper, and the timing of that decision, are instilled with a marked degree of irony. It also begs the question of whether it was constitutionally appropriate. On May 13, 2004, some ten days before it called an election, the government announced the creation of an Interim Committee of Parliamentarians on National Security to consider its consultation paper on that very subject. This was not done in the House of Commons, as one might have expected, but through a news release issued by the Government House Leader and Minister Responsible for Democratic Reform, which not surprisingly went unnoticed.[46] Whether it made that decision before it had decided to go to the polls is unclear. The result, nevertheless, was to permit a small group of parliamentarians under Liberal Party control to study the consultation paper and formulate recommendations within the government's original time frame. To this end a special government order was passed to permit the Privy Council Office to fund a limited amount of travel to Australia, the United States, and Britain during the summer of 2004 without parliamentary sanction.[47] After meeting in private with witnesses and with no official transcripts being made for public consumption, this committee duly submitted its report to the deputy prime minister in time for the fall session of Parliament beginning in October.

REPORT OF THE INTERIM COMMITTEE

Like the consultation paper the Interim Committee's report is not without flaws. It too only considered oversight mechanisms among Canada's primary intelligence partners, and there is little indication concerning what the committee learned there. Though it did have meetings with certain academics, these were all from outside Canada. Given the perspectives that could have been provided by those who had worked for the McDonald Commission—particularly those broadly knowledgeable about parliamentary practice—or more recent committee processes, this was unfortunate. But perhaps the greatest weakness of the committee's report lies in its failure to confront head-on the recommendations and positions advocated in the government's consultation paper. Clearly this was a political document that demanded a political response. From that perspective the Interim Committee needed to identify the flaws in the British model from a parliamentary perspective, and this it did not do. Nor did it identify how in previous embodiments it had been unable to fulfill its constitutional or statutory mandates.

Instead the Interim Committee looked at the issue of parliamentary oversight in a rather detached, almost academic manner and through a quite different lens to that of the consultation paper. Its emphasis was on how best to scrutinize Canada's intelligence community, provide substantive accountability, and maintain the public's trust. Though cognizant of the need for safeguards and accepting of the premise that there were "probably significant parliamentary procedural and privilege issues that [would] need to be resolved by procedural experts and legislative drafters," it did not believe these were insuperable.[48] Not surprisingly, therefore, it came out firmly in favor of a committee of Parliament defined by statute, not a committee of parliamentarians. It argued that though such a committee would provide "thorough and comprehensive scrutiny" of Canada's intelligence community, it must be both independent of the Executive, and be seen to be so, if it were to maintain the trust of Canadians and the confidence of Parliament. This would in part be achieved by having a defined relationship with extant and future review bodies that would require them to report to Parliament through the new committee. It was careful, however, to stress that neither this process nor any other facet of parliamentary scrutiny of intelligence should "derogate from Parliament's privilege to send for people, papers and records, or diminish the role and authority of any other parliamentary committee."[49] Unfortunately for the credibility of the committee, it exhibited a tendency to demand the best of all worlds, arguing that while it should enjoy all the rights and privileges of Parliament, it should also enjoy additional rights and privileges not permitted regular standing and special committees.

Much to the chagrin of many of the Interim Committee's members, the deputy prime minister refused to make its report public for study by Parliament and others until April 2005. At that time the government announced it would follow the advice of its own consultation paper and establish a committee of parliamentarians. Again the lexiconic sleight of hand was repeated in a government news release: "The proposal builds on the commitment set out in the National Security Policy and the Action Plan for Democratic Reform."[50] In fact, it detracted from the prime minister's initial proposal, and had in the process cynically used parliamentarians to give it a semblance of credibility.

THE EVENTUAL LEGISLATION

It would, in fact, be a further six months before the government would table legislation. Needless to say, Bill C-81 completely ignored the recommendations of the Interim Committee and followed the model laid out in the consultation paper.[51] Arguably its draft legislation was defective in several important respects. First, there was no clear relationship between extant review bodies and the new committee. Thus it was, for example, unclear whether the committee would have access to material in the hands of the various review bodies at any point during the year. Second, though the mandate of the committee appeared to be open-ended

and of wide span, its work could easily be limited. Not only was it obliged to "request" information of the minister, but the minister retained total discretion to limit what the committee could see in several important respects. Third, the government would have retained control over the committee's reporting capacity to Parliament. Only one opportunity each year was perceived necessary, and that was through the committee's annual report. Even the British model has greater capacity than this. And, unlike SIRC, it retained no right to the final say on what went into its reports. Fourth, the distrust with which current parliamentarians are viewed was confirmed by making them subject to the Security of Information Act for life. It should be noted that members of SIRC are not so bound. For them it was thought that a privy councillor's oath would suffice. Finally, the committee's resources were not clearly identified in the legislation. However, the backgrounder document, which accompanied the bill, did indicate that it would be provided with security-cleared staff from within the government's security and intelligence community. The British example has shown that such an approach has definite limitations.

There is one contextual issue that may have had bearing on the decision to opt for a committee of parliamentarians, but this is an issue so sensitive that it is never openly discussed by the politicians. Any committee of Parliament would necessarily have to include members from all official parties in the House—including the *Bloc Québécois* (BQ). Since the latter is a party fundamentally committed to promoting the secession of Quebec from the federation, and this directly challenges the integrity of the national state, there is a clear difficulty in permitting BQ members to participate in a security-cleared committee dealing with the security of the national state. So serious is this difficulty that in the case of SIRC, no BQ representative has ever been appointed, even when the BQ formed the Official Opposition in Parliament from 1993 to 1997, and despite the fact that all other officially recognized parties have had appointments to SIRC from their ranks. Yet the political sensitivity is such that there has never been any official acknowledgment of this apparent anomaly.[52] A committee of parliamentarians, on the other hand, neatly finesses this difficulty, as the prime minister would not be bound to appoint any BQ as a member of Parliament. Yet no public notice was ever given concerning this point.

CONCLUSION

The legislation died a natural death with the defeat of the government at the December 2005 polls. A new but Conservative minority government is now in office under Stephen Harper. Already it has used an interim committee of parliamentarians to consider the appointment of a new Supreme Court Justice, the mechanism recommended by the Justice Committee in the last Parliament. Also, it apparently has new but obscure ideas on how to attend to matters in the security and intelligence portfolio. These include expanding Canada's foreign intelligence

capacity in some way, the new but unexplained office of National Security Commissioner, and a National Security Review Committee. In the latter regard, it is unclear whether this will merely be an expanded version of SIRC, some form of parliamentary body, or some new innovation altogether.

By way of a conclusion it is therefore timely to consider what Parliament needs if it is to play its constitutional part in holding ministers to account in this important area of government. First and foremost, without access to secret information on a regular basis, Parliament cannot know what questions are appropriate to ask ministers if they are to hold them accountable in any significant manner. There is no reason, for example, why a small group of parliamentarians should not, subject to appropriate safeguards, be able to go to a secure location and view the latest all-hazards assessment of the threats that the government believes Canadians face. This will give MPs pause, perspective, and hopefully the capacity to ask important questions of the intelligence and security officials as well as responsible ministers.

By their nature parliamentarians are busy people. It may be anticipated that the amount of time they can devote to scrutinizing the security and intelligence community will be limited. They should, therefore, focus on what they can do best and not intrude or duplicate the work of the independent or internal review bodies. Of particular importance should be the bigger picture issues of policy, performance, capacity, and resources. This does not mean that parliamentarians should not be interested in the mandates or activities of the review bodies, especially where compliance is concerned. To the contrary, one of their primary jobs should be to watch the watchers on a regular basis. As a first order of business they should try to establish whether the review bodies are, in fact, doing the sorts of things that Parliament intended and whether there are holes in the mandates of the review regimes that are currently in place. To this end, they should have access to all the various reports and certificates that are currently produced by the intelligence collection agencies and their watchers, as well as the ministerial directions and authorizations given to the agencies. In addition, they should have timely access to the people involved, and be able to make suggestions about the work plans of review bodies.

A crucially important element in any committee required to scrutinize the national security sector will be the staff it hires. Such staff should be composed of people working on a full-time basis for the committee as well as individuals who can be called in to work for it on an as-required basis or as special advisors. In terms of expertise, it would be advisable to draw on, as the U.S. congressional committees have done, persons who have experience working for intelligence organizations as well as others with strong research, analytical, auditing, and legal capacities from other backgrounds. All will need to be security cleared to the highest top-secret level, will need to work in a secure environment, and will need to operate under oath.

It would be prudent that each report the committee intends to make public first be examined to ensure that nothing of a sensitive nature is untowardly

released. However, the committee should have the right, as SIRC does, to determine its final content. It should also be able to release reports in a timely fashion, not after months of delay.

To maintain the trust of Canadians and to contribute to a reduction in the democratic deficit, the committee will need both to be *of* Parliament and independent of the executive branch. Its powers and privileges of Parliament should not be circumscribed in anyway. However, any committee should be established by a statute that sets out: the size of its membership, how its members and chair are to be selected, the general mandate of the committee, the access it is to receive, the oaths that are to be administered, the security procedures that are to be followed, the staff and other resources it should have, and the relationships it should have with the extant review bodies. Significantly, it should be permitted to continue its work between sessions or when Parliament is prorogued.

NOTES

1. See, for example, John Starnes, "Review Versus Oversight," in A. Stuart Farson, David Stafford, and Wesley K. Wark, eds., *Security and Intelligence in a Changing World: New Perspectives for the 1990s* (London: Frank Cass, 1991), pp. 95–103.

2. Both the CSE and the commissioner would, however, remain without a statutory footing until the 21st century. For an analysis of how the CSE avoided public disclosure, see Stuart Farson, "So You Don't Like Our Cover Story—Well We Have Others: The Development of Canada's Signals Intelligence Capacity Through Administrative Sleight of Hand, 1941–2000," in Bob Menzies, Dorothy Chunn, and Susan Boyd, eds., *(Ab)Using Power: The Canadian Experience* (Halifax: Fernwood Press, 2001), pp. 78–94.

3. For a detailed assessment of the changes of both the Martin and Chrétien governments, see our chapter, "The National Security Policy Process," in David Dewitt, ed., *Canada and International Security*, forthcoming.

4. Numerous polls have indicated the lack of esteem with which Canadians hold their elected officials. A recent survey indicated a mere 14% of Canadians trusted MPs, below even car salespersons. See: Leger Marketing's survey, "Professional Barometer," March 19, 2006. Recently, only 36% of Canadians believed that the will of the people was being followed. See: Jill Mahoney, "Only One-Third of Canadians Feel Will of the People Rules, Poll Finds," *Globe and Mail*, April 3, 2006.

5. See: "Prime Minister Announces Appointment of Cabinet," *News Release*, December 12, 2003, p. 1, available at: http://ww1.pm.gc.ca/eng/news/asp?id=8; (accessed February 11, 2004).

6. See: ibid., p. 6, item 11.

7. His persuasive visit likely occurred sometime in January as an overture was made by the prime minister in January 2004 to opposition party leaders to swear them in as privy councillors "in order to facilitate them being briefed on sensitive information including in relations to the Arar matter." Material released under Access to Information Act.

8. See the "Statement of Work" component of the contract dated February 2, 2004. Emphasis added. This was released under the Access to Information Act on January 6, 2006, almost a full year after the request was made. The scope of work focused on

"defining and reviewing options for the mandate, structure, composition, support mechanisms and consultation processes for the new committee."

9. It is unclear why the government wanted to pursue such a tight time frame. One possible reason is that it wanted Parliament's input before that body would have to begin its three-year review of Bill C-36, the Anti-Terrorism Act, slated for December 2004.

10. "Deputy Prime Minister Tables Consultation Paper on National Security Committee of Parliamentarians," *News,* March 31, 2004, available at http://www.psepc-sppcc.gc.ca/publications/news/20040331-2_e.asp (accessed October 27, 2004).

11. *A National Security Committee of Parliamentarians: A Consultation Paper to Help Inform the Creation of a Committee of Parliamentarians to Review National Security*, Ottawa, 2004, available at http://psepc/sppcc.gc.ca/publications/national_security/nat_sec_cmte_e.asp (accessed October 12, 2004).

12. Ibid., p. 5.

13. Ibid., p. 5.

14. Ibid., p. 6.

15. Ibid., pp. 6–7.

16. Ibid., p. 7.

17. Maher Arar, a Canadian citizen of Syrian birth, is the best known victim of the American practice of "extraordinary rendition," whereby terrorist suspects are "rendered" to countries with dubious human rights records and methods of interrogation. Arar was detained at a New York airport in transit to Canada and, in contravention of international law and without Canadian knowledge, was sent to Syria where he was imprisoned and tortured before being released by his captors for want of any evidence against him. On his return to Canada, he became a *cause célèbre*, and a serious embarrassment to Canadian-American relations. The O'Connor inquiry was charged with examining the matter of the possible complicity of Canadian officials in his handling by the U.S. and Syrian authorities. The Americans refused to cooperate with the inquiry. The terms of reference and other information related to the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, which was established on February 6, 2004, may be found at http://www.ararcommission.ca/eng/index.htm.

18. *A National Security Committee of Parliamentarians: A Consultation Paper to Help Inform the Creation of a Committee of Parliamentarians to Review National Security,* pp. 8–9.

19. Ibid., p. 9.

20. Ibid., p. 14. Emphasis in the original.

21. Ibid., p. 16. Emphasis added.

22. See: Commission of Inquiry into the Actions of Canadian Officials Relating to Maher Arar, Policy Review, *Consultation Paper*, Ottawa, October 2004, available at http://www.ararcommission.ca/eng/Consultation_Paper_Oct5.pdf (accessed October 21, 2004).

23. The research papers are available on the commission's website at http://www.ararcommission.ca/eng/15.htm. One might also note that the commission's *Legal Framework* was also more comprehensive. This is available at http://www.ararcommission.ca/eng/Legal_Framework.pdf (accessed October 21, 2004).

24. A search for "parliamentary oversight" using the Google search engine yielded over 109,000 hits. See: http://www.google.com/search?sourceid=navclient&ie=UTF-8&q=Parliamentary+Oversight (accessed October 27, 2004).

25. Peter Gill, *Policing Politics*: *Security Intelligence and the Liberal Democratic State* (London: Frank Cass, 1994).

26. Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (Oxford: Clarendon Press, 1994).

27. This organization has held numerous international conferences and workshops on the theme of democratic control and oversight of security and intelligence organizations. Many of their papers may be found at http://www.dcaf.ch/index.htm. Recent efforts have focused on the need to develop a model law that democratic states of all constitutional stripes can employ. See particularly: Hans Born, Loch K. Johnson, Ian Leigh, eds., *Who's Watching the Spies? Establishing Intelligence Service Accountability* (Washington: Potomac Books, 2005), and Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practices for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005). See also their work with the Inter-Parliamentary Union, Hans Born (editor and lead author), "Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices," *Handbook for Parliamentarians*, No. 5 (2003).

28. See, for example, the website of the British Security Service at http://www.mi5.gov.uk/output/Page93.html and that of the Australian Department of Defence at http://www.dsd.gov.au/about_dsd/oversight.html (both accessed October 27, 2004).

29. See, for example, Frederick M. Kaiser, "Congressional Oversight," *CRS Report for Congress*, 97-936 GOV (updated January 2, 2001), CRS1-6.

30. Ibid., CRS-2.

31. See, for example, Joel D. Aberbach, *Keeping a Watchful Eye: The Politics of Congressional Oversight* (Washington, DC: Brookings Institution, 1990).

32. See: Paul C. Light, *Monitoring Government: Inspectors General and the Search for Accountability* (Washington, DC: Brookings Institution, 1993), especially p. 14.

33. See: John F. Bibby, "Congress' Neglected Function," in *The Republican Papers,* ed. Melvin R. Laird (New York: Anchor Books, 1968), pp. 477–88.

34. Ogul, *Congress Oversees the Bureaucracy*, pp. 4–8.

35. Mathew D. McCubbins and Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms," *American Journal of Political Science* 28 (February, 1984), pp. 165–79.

36. Ibid., p. 171.

37. Ibid., pp. 172–73.

38. Ogul, *Congress Oversees the Bureaucracy*, pp. 6–7. Emphasis added.

39. This assessment draws on: William J. Keefe and Morris S. Ogul, *The American Legislative Process: Congress and the States* (Englewood Cliffs, NJ: Prentice Hall, 1985), Chapter 12: "Legislative Oversight of the Bureaucracy," pp. 332–57.

40. Aberbach, *Keeping a Watchful Eye*, p. 46.

41. For example, between 1970 and 1982, congressional staff (personal and committee) increased by two-thirds to 18,761 (Christopher J. Bailey, *The U.S. Congress* [Oxford: Blackwell, 1989], p. 88). Over the decade 1970–80 committee staff alone increased by 126% to 3,026 (Stephen S. Smith and Christopher J. Deering, *Committees in Congress* [Washington: Congressional Quarterly, 1984], p. 205).

42. Aberbach, *Keeping a Watchful Eye*, pp. 102–4.

43. See Canada, House of Commons, Standing Orders, section 108.

44. Transcripts of committee hearings are not recorded outside of Canada. The quotation is taken from the authors' personal notes.

45. For details of the difficulties experienced by the special committee, see: Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" in Philip Stenning, ed., *Accountability for Criminal Justice* (Toronto: University of Toronto Press, 1995), pp. 185–212.

46. See: Office of the Leader of the Government in the House of Commons, "Establishment of an Interim Committee on National Security," available at http://www.pco-bcp.gc.ca/lgc/default.asp?Language=E&Page=archive&Sub=press&Doc=20040514_secur_e.htm (accessed April 4, 2006).

47. Tim Naumetz, "Parliament May Become Watchdog," *National Post*, August 18, 2004, p. A4.

48. See the transmittal letter from Derek Lee and Senator Colin Kenny of October 4, 2004, submitting the report to Ms. McLellan, released under Access to Information Act.

49. Ibid.

50. See: "Model for National Security Committee of Parliamentarians," April 4, 2005, available at http://www.psepc-spepc.gc.ca/media/nr/2005/nr20050404-1-en.asp (accessed April 3, 2006).

51. Bill C-81 An Act to Establish the National Security Committee of Parliamentarians, First Reading November 24, 2005.

52. Curiously, the BQ itself has never drawn attention to its exclusion from SIRC, perhaps out of a realization that any public attention would only serve to indicate to their constituents that BQ members could not fulfill all their functions as federal MPs.

5

SOURCES AND METHODS IN THE STUDY OF INTELLIGENCE

A British View

LEN SCOTT

REPUTEDLY, "MAY YOU LIVE IN INTERESTING TIMES," is an ancient Chinese curse. The study of intelligence in the first years of the 21st century occurs in interesting times that show no sign of becoming less interesting. The role of secret intelligence in international security and world politics is now more prominent than ever in Western politics. Public expectations of intelligence have never been greater, and these include disclosure of the role of secret services. In the United Kingdom much of this has been generated by the terrorist attacks of September 2001 and July 2005, and by the war on Iraq. For many, the attacks brought home the vulnerability of Western societies and the importance of reliable intelligence on terrorist threats. Yet the war on Iraq raised doubts about the competence and reliability of intelligence and, moreover, the extent to which politicians had corrupted intelligence processes to serve predetermined political goals.

Though British and American intelligence share common purposes and common heritages, attitudes toward the disclosure of intelligence in the two countries have been markedly different. In the United States, freedom of information legislation and respective presidential initiatives have enabled scholars and citizens to scrutinize the record of U.S. intelligence agencies and their role in the policy process. There remain constraints on sources in the United States, and evidence of systematic reclassification of national security documents since 1999 has led to complaints of "declassification in reverse."[1] There are those who argue that American declassification policies are far too restrictive, and serve to fuel conspiracy theories about the U.S. government.[2] Yet by comparison with other liberal democracies, the American approach to declassification remains the exemplar of glasnost, and has laid the foundation of a corpus of literature that provides for understanding and debate on intelligence far exceeding that of any

other polity. The culture of greater openness permeates into memoir and testimony that inform, corroborate, and challenge archival-based interpretations. The British experience is very different and stands as a useful corrective for those who take for granted their understanding of the secret world and who may not reflect on the limited and problematic nature of their knowledge.

Better understanding of the intelligence process and its importance to national and international security has never been more necessary. Nor has the need to grasp the limitations as well as the value of intelligence.[3] In Britain, these challenges occur against a background of two decades of changing official attitudes and increasing opportunities in areas of archival disclosure. This chapter assesses some of these challenges and opportunities for the study of intelligence in the United Kingdom and places them in historical context. It focuses on various aspects of intelligence organization and practice, specifically covert action and central intelligence machinery. And finally it reflects on the extent to which recent events pose new challenges to the study and practice of British intelligence. The focus is on the study of British intelligence, although many of the issues are generic in nature and many intelligence scholars in the United Kingdom have written on other polities and experiences. The aim is not to provide a historiographical overview, though some key texts and authors are identified.

SECRECY, OPENNESS, AND ACCOUNTABILITY

Modern-day students (particularly from North America) may find it difficult to comprehend the culture of secrecy that pervaded all aspects of British intelligence (as well as other aspects of state activity) for most of the 20th century.[4] Secrecy precluded any meaningful form of parliamentary or public scrutiny, save for occasional political crises involving intelligence. In 1924 Foreign Secretary Sir Austen Chamberlain solemnly told the House of Commons, "It is of the essence of a Secret Service that it must be secret, and if you once begin disclosure it is perfectly obvious . . . that there is no longer any Secret Service and that you must do without it."[5]

This attitude, underpinned by the 1911 Official Secrets Act, aimed to prevent disclosure of any kind. This was not always successful. Indeed, only three years after the foreign secretary delivered his strictures to Parliament, he and the prime minister stood in the House of Commons reading out decrypted Soviet telegrams to justify breaking off diplomatic relations with the Soviet Union (and at a stroke sabotaging the efforts of British signals intelligence against the Soviets for decades). Nevertheless, until the late 1980s, British governments, both Conservative and Labour, resolutely sought to preserve the convention of all-embracing secrecy in matters of security and intelligence.

This did not prevent people from writing about intelligence. Various spy scandals involving Soviet espionage fueled and sustained public interest and

speculation. The saga of the "mole-hunts" verged on a national obsession. British intelligence was depicted as unsuccessful and incompetent. That portrayal was soon countered by revelations from former officers involved in wartime triumphs against the Germans kept secret for nearly thirty years. In 1972 Sir John Masterman published an account of British counterintelligence and the Double Cross committee in World War II.[6] This had been written as an in-house history in 1945, and was published by the 80-year-old author "to give credit to those [intelligence officers] who deserved it" as well as to help rehabilitate the reputation of British intelligence after the debacles of the moles and mole-hunts of the postwar period. In 1974 Group-Captain Fred Winterbotham published an account of ULTRA based on his recollections as the senior Air Staff representative in the Secret Intelligence Service (SIS/MI6).[7] One consequence of these two accounts was that they contributed to the climate of opinion in which the official histories of British intelligence in World War II were sanctioned.

Espionage had already emerged as a literary genre earlier in the century. The Cold War provided fertile ground for some of the most absorbing representations of espionage, notably in the novels of former intelligence officer John Le Carré. Intriguingly, notwithstanding legal prohibition on disclosure, many former officers found ways to write about the subject, at least in literary format. According to Nigel West, "It is one of the paradoxes of the British intelligence tradition that whereas there is a convention, and now a criminal statute, to prevent intelligence officers from making unauthorised disclosures, more have done so in this country than anywhere else in the world."[8] Yet in 1986 the Thatcher government sought to prevent disclosures by former Security Service (MI5) officer Peter Wright, in his book *Spycatcher*.[9] Wright made sensational and embarrassing allegations that the former director-general of MI5, Sir Roger Hollis, and the former prime minister, Harold Wilson, had been suspected (by some intelligence officers) of working for the KGB. Wright had retired to Australia, where the British government brought a civil suit based on the breach of duty by a servant of the Crown (rather than a breach of the Official Secrets Act). The case was nevertheless lost and brought into ridicule official British attitudes toward disclosure. The fiasco was one element in changing attitudes toward unnecessary secrecy. It also fueled the animus of specialist intelligence writers who were derisively dismissive of intelligence.[10]

Writing in 1988, the most prominent British intelligence historian, Christopher Andrew, inveighed at Whitehall's obsession with "the continued overclassification of ancient secrets," but nevertheless noted that the volume of reliable information about the current intelligence community had increased to "at least a trickle."[11] Since then important changes have taken place. All three security and intelligence organizations (the Security Service, the Secret Intelligence Service, and Government Communications Headquarters [GCHQ]) have been placed on a legal basis and a form of parliamentary oversight was established in 1994. Until the 1990s official British attitudes toward secrecy aimed to prevent any disclosure whatsoever. Indeed, it was not until 1992 that the British

government publicly acknowledged the existence of the Secret Intelligence Service in peacetime.[12] Until then, as Gill Bennett, the chief official Foreign Office historian explains, this meant that any record that even mentioned SIS was withheld.[13] Changes in disclosure were eventually followed by changing attitudes to parliamentary accountability. When placing the Security Service on a statutory basis, the Conservative government of Margaret Thatcher rejected the principle of accountability. In 1994, however, her successor, John Major, created the Intelligence and Security Committee (ISC) as a committee of parliamentarians (not a parliamentary committee) appointed by the prime minister to examine the expenditure, administration, and policy of the three security and intelligence services.

Critics and skeptics have queried the motives for reform. How far change was driven by the legal requirements of European human rights legislation rather than by changes within Whitehall or within the intelligence and security services is a matter for debate. Peter Gill argued that changes toward accountability reflected primary concern with information control and that the state had "shifted its ground from traditional assertions of an absolute right to secrecy in any matter that can be labeled 'national security' to a more subtle strategy mixing secrecy and persuasion" that had "more to do with public relations than with any genuine advance in accountability."[14] The development of the ISC fell short of fully fledged parliamentary accountability afforded by the system of select committees. Nevertheless, its role has evolved, moving gradually beyond its original remit. Aspects of the committee's performance over Iraq and its aftermath have been criticized, though it continues to undertake investigations and reports into aspects of contemporary intelligence that are a helpful source for students of the subject. A further dimension of increasing parliamentary scrutiny is the European Parliament's growing interest and concern with intelligence issues evidenced by its report on the U.S.-U.K.-Commonwealth ECHELON Interception system and by its investigations into allegations concerning secret CIA detention centers in Europe.[15]

John Major's Open Government Initiative in 1992 augured a process of change in declassification. In 1997 the records of the Security Service began reaching the Public Record Office (now the National Archives). Subsequently, the files of GCHQ began to be transferred to the National Archives, and the wartime records of the Government Code and Cipher School (GCHQ's predecessor) are now open. GCHQ also undertook joint declassification of the VENONA operation, providing details of Western decryption of Soviet cipher communications. In common with the Security Service, a policy governing selection of GCHQ records has been agreed with the National Archives and approved by the Lord Chancellor's Advisory Committee on Public Records.[16] SIS did facilitate the opening of the wartime Special Operation Executive (SOE) records. SIS archives themselves are not declassified, although there is apparently cooperation with other government departments to allow greater release of SIS papers held in their departmental files.

Other changes in declassification procedures have advanced the cause of openness. Government departments, where possible, now extract or redact sensitive material rather than withholding the entire document. Most recently, in 2005, the Freedom of Information Act came into force. Although the intelligence agencies are excluded from the act, documents held in other departments' files are covered by the legislation. Time will tell whether this yields interesting results.

SOURCES AND METHODS

Until the 1980s British academic interest in the study of intelligence was limited mostly to a small number of historians. In 1984 Christopher Andrew and David Dilks invoked Sir Alexander Cadogan's description of intelligence as the missing dimension of international affairs.[17] In 1986 Andrew cofounded *Intelligence and National Security,* which is now firmly established as the leading international journal in the field. The development of intelligence studies as a subfield of international relations has continued to gather momentum ever since. And this momentum has been accelerated by changes in declassification policies and attitudes toward secrecy.

Notwithstanding the traditional British culture of secrecy, British intelligence records have been accessed in a variety of ways, including official histories, discreet collaborative arrangements, ad hoc collections of documents, and published in-house histories.[18] Unauthorized disclosure provides further dimensions to our understanding. Official histories of British intelligence in World War II appeared after 1979 and provided highly detailed and authoritative accounts. They were nevertheless restricted to the war against the Axis powers, and no attempt was made to explore the penetrations made by Soviet intelligence before and during the war. The final—and arguably most compelling—volume, on strategic deception, was completed in 1980 but not published until 1990 because of Prime Minister Thatcher's anxieties.[19] Though the work of F. H. Hinsley's team is commonly described as magisterial, some knowledgeable insiders were rather more critical. The former chief of SIS, Sir Maurice Oldfield, is reported to have described the first volume as "a book written by a committee, about committees for committees."[20]

What is clear is that no attempt has been made to repeat the exercise, although Richard Aldrich has argued the case for a comparable study of Cold War intelligence.[21] When the Security Service decided to sanction a history of MI5 to mark the centenary of British intelligence, they chose Professor Christopher Andrew of Cambridge University to undertake the project on a part-time basis. After some procrastination, SIS followed suit with the appointment of Professor Keith Jeffery of Queens University, Belfast, who has been commissioned to write a volume of SIS official history covering 1909 to the early Cold War for publication in 2010. Both historians have access to service archives, though SIS's recently created website is keen to emphasize that commitment to the protection

of intelligence sources remains paramount and the book will not reveal operational details that remain sensitive.[22] In a similar vein, the recent *Official History of the Falklands War* by Sir Lawrence Freedman draws from and refers to the British Joint Intelligence Committee (JIC) assessments but provides nugatory insights into the activities of SIS or GCHQ.[23]

Other initiatives have taken place. In 1997 the Foreign Office published documents covering the mass expulsion of Soviet intelligence officers from Britain in 1972.[24] The Foreign Office also commissioned an evaluation of the Zinoviev Letter by their chief official historian, which drew from SIS files as well from Soviet records made available by the Russian government.[25] Some British writers have gained access to prewar SIS records on an ad hoc basis. Gordon Brook-Shepherd used SIS files for his study of Western intelligence and the Bolshevik revolution, where *inter alia,* he traced SIS involvement in the plot to overthrow and assassinate Vladimir Lenin.[26] Alan Judd was similarly aided in his biography of the first chief of SIS, Sir Mansfield Cumming. More recently, Andrew Cook was given access to SIS records for his biography of the famed SIS officer, Sidney Reilly.[27]

British intelligence has also facilitated publication of books designed to illuminate the operations of Soviet intelligence during the Cold War. In 1990 Oleg Gordievsky, a KGB intelligence officer who worked for SIS as a "defector-in-place" for eleven years, published an account (with Christopher Andrew) of KGB operations, which, *inter alia*, made clear the identity of the "Fifth Man" of the mole-hunt saga (John Cairncross).[28] In 1999 Vasili Mitrokhin and Christopher Andrew published an account of KGB operations in Europe based on copies of KGB documents made by Mitrokhin, a KGB archivist, which was exfiltrated from the USSR by British intelligence in 1992.[29] A second volume, dealing with KGB global operations was published in 2005.[30] It is an axiom that success in intelligence remains hidden whereas failure is publicized. These books are clearly intended to illuminate British intelligence success as well as the nature and scope of their adversaries' activities.

Intelligence records exist elsewhere than in the archive of intelligence services. Christopher Andrew has long maintained that opportunities exist for archival research using "adjacent files" of departments such as the Foreign Office and the Home Office.[31] Moreover, evidence of joint intelligence activities or information supplied to allies may be found in the archives of those allies, including those of the British Commonwealth. Similarly, much SOE material was discovered in the American National Archives after the files of the Office of Strategic Services were deposited there in the 1980s. An additional value of such depositories is that they may contain materials that not have been retained or were indeed destroyed by the original service.

Finally, one potential source is that of an adversary's archives. Material destroyed, withheld, or lost may eventually surface in the archives on the other side of the hill. A fascinating recent example is the publication of the minutes of a joint SIS/CIA planning meeting in 1953 for the operation to intercept Soviet

communications in Berlin. The document was supplied by the KGB's agent in SIS, George Blake, copied from the Soviet archive by Sergei Kondrashev (Blake's case officer in 1953), and published in 1997 in a collaborative venture by Kondrashev and former CIA officers.[32] Similarly, Nigel West and Oleg Tsarev provide an account of materials in the KGB archive acquired by Anthony Blunt and Kim Philby, based on Tsarev's access to the files.[33] One significant innovation in the study of Cold War intelligence archives is the work of Paul Maddrell in using the records of the East German *Stasi* to gather evidence of Western intelligence activities.[34]

Notwithstanding different national patterns of declassification and disclosure, all intelligence services adhere to the principle of protecting sources and methods. Gill Bennett, for example, argues that "the principal reason why the CIA has released so much material is that the form and content of its records have made it possible to do so."[35] SIS, she contends, pursues the same policy as that of the CIA in protecting its sources and agents. Yet how the principle is applied may vary. In 1992 the CIA released documents detailing operational aspects of the joint CIA-SIS Penkovsky case that included operational plans, transcripts of debriefings of Penkovsky conducted by CIA and SIS case officers, and maps of signal sites and dead letter drops.[36] It is difficult to imagine SIS declassifying any such materials. Though duties of care to the families of agents may necessitate withholding their identity long after their death, can the same apply to methods? Certainly one reason why the British did not wish to disclose the ULTRA secret after 1945 was that the ENIGMA machines were used after the war by other states. Yet there is surely much in Wesley Wark's caustic comment, "It is to be profoundly hoped that 'intelligence methods' employed before 1914 have not remained so constant as to require genuine protection as a matter of national security."[37]

COVERT ACTION

Though much contemporary study of intelligence concerns how knowledge is acquired, generated, and used, some intelligence services secretly intervene in the affairs of other states or political actors. As Richard Aldrich puts it: "Operations to influence the world by unseen means—the hidden hand."[38] The "hidden hand" is not always wielded by intelligence services. In Britain the Information Research Department (IRD) of the Foreign Office performed various propaganda activities, and these have proved now amenable to archival exploration. Research into IRD has also contributed to the development of cultural or public diplomacy—one of the emerging trends in Cold War historiography.[39]

Terminology to describe secret intervention by British intelligence has moved from "special operations" to "special political action" to "disruptive action."[40] The semantic changes reflect broader shifts in policy. The special political action of the 1950s, for example, was synonymous with overthrowing governments and, in some cases, assassinating leaders.[41] Since then, changes in the scope and nature of

operations have reflected changing priorities and perspectives. Although the Intelligence Services Act 1994 makes clear that SIS's mandate is to engage in "other tasks" beside espionage, the scope and nature of these other tasks is unclear.[42] Mark Urban provides an account of SIS's role in Afghanistan in the 1980s in supporting one of the *mujahedeen* leaders, Ahmed Shah Massoud, against the Soviets.[43] In a different vein, SIS (and MI5) was involved in developing lines of communication to the Provisional Irish Republican Army in the 1990s that helped facilitate the Northern Ireland peace process.[44] The scope of "other tasks" is nowhere listed.

Covert action raises a variety of potential political, legal, and ethical controversies and their disclosure has often come from unauthorized sources. The SIS whistle-blower, Richard Tomlinson, has indicated that SIS is required to "maintain a capability to plan and mount 'Special Operations' of a quasi-military nature" that are "executed by specially trained officers and men from the three branches of the armed forces."[45] Tomlinson asserts that SIS engaged in assassination planning against the Serbian president, Slobodan Milosevic, that it endeavored to disrupt the Iranian chemical warfare program, and that it acted as an instrument of the CIA in defaming UN Secretary-General Dr Bhoutros Bhoutros Ghali.[46] David Shayler, the former MI5 whistle-blower (who like Tomlinson was imprisoned for breaches of the Official Secrets Act), has stated that SIS supported groups seeking to overthrow and assassinate the Libyan leader Colonel Ghaddafi in 1995/6, and what appears to be SIS documentation has been posted on the internet providing apparent corroboration.[47] Lack of clarity about the term "disruptive action" reflects the determination of the British government to avoid disclosure of some of the activities involved.

In his detailed study of SIS, Stephen Dorril argues that far more information is in the public domain than anyone has realized and that "the reality [is] that secrets are increasingly difficult to protect, and it would not be a great exaggeration to suggest that there are no real secrets any more."[48] Yet comparison between American and British attitudes toward disclosure of covert action is apparent, and noticeably so where the two have been jointly involved. An interesting example concerns the operation conducted by the CIA to overthrow the government of Iran in 1953. In 1998, after a legal tussle, the CIA partially declassified an account of the operation written by Scott Koch of its history staff.[49] The document was very heavily redacted and of limited value to historians. Notwithstanding declarations from several CIA directors, and notwithstanding opening of CIA files on other operations, there was very limited progress on Iran. One reason was that a large numbers of files were destroyed in the 1960s. Another was the fact that the operation was conducted in cooperation with the British government. Koch's account (or at least the nonredacted parts) omitted discussion of British intelligence, though it includes a passing reference to the published account of the erstwhile SIS head of station in Tehran (who is erroneously referred to as belonging to MI5).[50]

However, the *New York Times* received a copy of a contemporaneous in-house CIA history from a former official and published several articles in April 2000 based on this. In June the near-200-page document itself was posted on the

internet. The account was written in 1954 by the CIA's Dr Donald Wilber, who was intimately involved in planning the operation.[51] Attempts were made to digitally black-out names of individual Iranian agents, but according to the National Security Archive, the method of redaction could be circumvented to allow their identification. A revised method of redaction was then employed and the resulting document appeared on both the *New York Times* and National Security Archive websites.[52] The 1954 CIA report provided insight into the British role, including the identity of British secret service officers and agents, details of Foreign Office involvement, and the 29-page outline plan for the operation prepared by SIS for the Americans.

Particular kinds of covert action may present particular challenges in establishing a paper trail. No written record, for example, has emerged of presidential authorization of CIA-sponsored attempts to assassinate Fidel Castro. Archival release does sometimes provide evidence of political involvement, and evidence has emerged that President Eisenhower authorized the assassination of Patrice Lumumba, the prime minister of the Republic of Congo.[53] In Britain, various accounts refer to the role of SIS in coup plotting and assassination planning, particularly in the Middle East, and a clear historical consensus exists on these activities in a variety of postcolonial contexts. The enthusiasm of Prime Minister Eden and of elements within SIS to assassinate President Nasser is evident, though archival corroboration has yet to appear. More recently, the private papers of former Defence Secretary Duncan Sandys have provided evidence of joint planning in 1957 by SIS and CIA to overthrow the Syrian government, involving targeted assassination of key leaders.[54] The approval of Prime Minister Macmillan for such measures is clear.

Specific operations may leave no paper trail or even any indication of their existence. One intriguing case concerns former British Prime Minister Callaghan's assertion that in 1977 he briefed the chief of SIS, Sir Maurice Oldfield, on British naval deployments in the South Atlantic in anticipation of an Argentinean threat against the Falkland Islands.[55] At the time there was concern within the British government that the Argentinean military *junta* might be preparing to use military force to resolve the disputed claims over sovereignty of the islands. The prime minister did not instruct the chief of SIS to pass on this information but hoped that he would and believed that he did. When the Franks Committee into the Falklands War investigated, SIS found no record of the operation.[56] So either Oldfield did not pass the information to the Argentineans (as Foreign Secretary David Owen believed[57]) or there seems to be no archival record of an operation that the prime minister believed was important in deterring a war in 1977.

UNDERSTANDING INTELLIGENCE MACHINERY

The self-image of British intelligence professionals is that of turning information into wisdom and speaking truth unto power (although the truth may often be

cautious, nuanced, and tentative). Understanding the conceptual and organizational dimensions of intelligence is central to understanding British intelligence. A sophisticated exponent of this view has been Michael Herman, writing on the basis of twenty-five years of experience at GCHQ and the Cabinet Office. A former secretary of the JIC, Herman has received wide acclaim for his expositions on the process of intelligence and has been described as "a historian and philosopher of intelligence."[58] *Intelligence Power in Peace and War* is a distillation of a lifetime's work and reflection, and remains a singular text in the British literature in proffering the kind of conceptual oversights familiar to American students of the subject. One key purpose is to characterize intelligence as a form of power in international politics. Elsewhere in Herman's writing he is equally notable for his attempts to focus on the ethics of intelligence. This concern predated September 11 and its aftermath.[59]

In Britain serious engagement with the ethics of intelligence has gained momentum, both from ethicists and former senior officials.[60] This engagement occurs as the debate between security and human rights has loomed large in the wake of terrorist attacks and attempts by the Blair government to strengthen the hand of the security services at the expense of traditional legal safeguards. Accusations of British collusion with the American denial of human rights in Guantánamo Bay and with CIA practices of "rendition" in Europe have furthered the potential engagement of intelligence with ethical (and legal) discourses in the United Kingdom.

Although an advocate of broadening the scope of the subject, Herman's primary aim is to promote greater public understanding of intelligence. Yet, in engaging with critical issues about the practice of the intelligence process, Herman seeks to legitimize intelligence and proselytize organizational approaches to the subject. The latter goal is shared by other writers, notably Philip Davies, whose work on SIS illustrates that changing attitudes toward disclosure have aided political scientists and their application of sophisticated organizational and management theories to understanding intelligence machinery.[61] Davies's work is important in highlighting the need to understand structure and process in assessing the effectiveness of British intelligence. This comes at a time when the Butler report focused on arrangements for validation and quality assurance in SIS (and the JIC) as a factor in what went wrong over Iraq.[62]

Other British intelligence mandarins have shared the goals of education and legitimization, notably Sir Percy Cradock, former Chairman of the JIC. The work of both Herman and Cradock epitomizes the prevalent self-image of the intelligence mandarin as providing objective, "policy-free" analysis to decision makers. Cradock's characterization of the JIC and its staff as "having an eye always to the future and to British interests, and free from the political pressures likely to afflict their ministerial masters" reflects the self-image of the intelligence community as guardian of the national interest against transient and feckless politicians. "Speaking truth unto power" has been the cornerstone of both the structure and the culture of British intelligence. Lord Butler's examination of the JIC's performance

over Iraqi weapons of mass destruction (WMDs) provides general vindication of the British system, though it also highlights specific areas where the confidence of the assessment was insufficiently supported by the strength of the intelligence.

Declassification of the JIC records began in the wake of John Major's Open Government Initiative with the first tranche of postwar records reaching the National Archives in the mid-1990s. To ensure the release of JIC material was in conformity with the thirty-year rule governing transfer of historical material to the National Archives, the Cabinet Office initiated an accelerated release process with JIC records dating from 1975 now available at the National Archives. Although this has yielded considerable insight into the formation of foreign and defense policy, the process by which the JIC assessments were reached is less clear. Critics of the JIC have complained that its conclusions were often anodyne and consensus-driven. The recent release of JIC secretariat records will allow scholars to analyze the background discussion to these minutes and illuminate hitherto unexplored aspects of decision making within the U.K. intelligence community.

It is nevertheless worth contrasting historical records of the JIC with recent exposure of the British intelligence machinery in the furore over Iraqi WMDs. Inquiries by the House of Commons Select Committee on Foreign Affairs, the Parliamentary Intelligence and Security Committee, Lord Hutton, and Lord Butler have provided unprecedented coverage and insight into British intelligence machinery.[63] These inquiries and reports provide unparalleled opportunities for the study of contemporary issues. Not only have specific paragraphs from JIC papers been published, but the role of constituent elements of the JIC assessment process have been exposed. In particular, the claims made by the government concerning the ability of the Iraqis to use chemical weapons within forty-five minutes have illuminated the role of the Defence Intelligence Staff (whose experts were not shown material provided by SIS from a key source). Our understanding has been greatly informed by the testimony and cross-examination of Whitehall officials as well as by written records including internal e-mails. In this context, an important counterfactual question can be posed: If we had not had these inquiries and historians had only gained access to JIC papers in thirty years' time, how would their accounts compare to those that can be constructed now? The question also illuminates the problem of relying on the archive alone. For historians in cognate areas of foreign and defense policy, interviews and personal recollections are indispensable in understanding and building upon the written record.

BROADER PERSPECTIVES AND SPECIFIC AGENDAS

The study of intelligence concerns the relationships among power, knowledge, and secrecy. In particular, it concerns the relationship between certain

kinds of power and certain kinds of knowledge. Differing approaches to the study of power and knowledge have long characterized theoretical debates about international relations, and recent development of poststructuralist and social constructivist discourses poses new challenges and presents new opportunities. Though many theoretical debates may loom as esoteric and self-referential to practitioners, there is potential relevance in theoretical approaches.[64] One notable example is Andrew Rathmell's essay on the potential importance of postmodern theorizing to the practice of intelligence.[65] Rathmell argues that intelligence services need to make radical changes in conceptual approaches and organizational structure to adapt to emerging social, cultural, and technological conditions and the "knowledge intensive, dispersed globalized systems." What he calls the "fragmentation" of threat requires different conceptual approaches to understanding security threats and radical changes in the way intelligence services collect and process knowledge about them. The epistemological assumptions of postmodernist thinking are wholly at variance with contemporary thinking in the American military, where the quest for perfect battlefield knowledge is the goal of those who proselytize the revolution in information warfare. What is of note about Rathmell's approach is that it explicitly seeks to make the most abstract of theoretical approaches policy-relevant. Recent events, most notably those of September 11, 2001, and July 7, 2005, provide a context in which thinking outside traditional boxes is necessary. Nevertheless, poststructuralist approaches to epistemology problematize knowledge at a time when conspiracy theories are readily generated and accepted, and when the search for objective assessments is necessary for those who wish to enhance the credibility of intelligence. Potentially more fruitful, perhaps, is the concern of social constructivism with identity, and the relationship between identity and power, which are clearly of potential relevance to understanding the nature of threats.[66] Identity is equally crucial to examining conflict and community in Iraq or indeed the beliefs and values of Muslims in modern Western states. In Britain, as elsewhere, there has been limited engagement between international relations theory and the study of intelligence.

Nevertheless, changes in some areas of theory parallel changes in practice. Recent developments in the study of security have attempted to move beyond an exclusive concern with military dimensions and conceptions of security. The study of intelligence, with its focus on the identification and interpretation of threat, and on the architecture of threat perception, has much to offer and much to gain from greater engagement with new approaches to security. In the post–Cold War interregnum of the 1990s an explicit intelligence agenda ranged from economic security to environment to health to organized crime, as well as to more traditional areas of arms transfers, WMD proliferation, and UN peace-keeping and peace-enforcing. Changes in world politics since the end of the Cold War created greater awareness of the importance of these issues. The "war on terror" and the continuing imbroglio in Iraq underline the need for deeper understanding of relevant global, regional, and local political and social forces.

DISCLOSURE, ACCOUNTABILITY, AND MANIPULATION

The war on Iraq has focused on the relationship between politics and intelligence on both sides of the Atlantic (and indeed elsewhere). Accusations of the politicization and manipulation of intelligence have been the subject of inquiries that provide considerable amounts of information about the intelligence process as well indeed the substance of intelligence. For the British government to discuss and evaluate its specific HUMINT sources in Iraq would have been almost inconceivable even a few years ago. The inquiries on both sides of the Atlantic have not surprisingly fueled public and scholarly debate, including about the nature and extent of official disclosure of intelligence material and assessments. Christopher Andrew has observed that "the threats posed by Osama bin Laden and Saddam Hussein [have] succeeded in transforming British government policy on the public use of intelligence."[67]

Nevertheless, the focus of disclosure and debate has concerned highly technical issues of weapons development and how this was presented to political leaders and by political leaders. Yet the issue of Iraq's development of WMDs was only one issue informing the decision to go to war. With the continuing problems in constructing a viable Iraqi state and the ongoing threat of civil war in Iraq the prewar estimates of what would happen after the invasion are likely to attract greater attention. The role of the JIC in this was not part of the terms of reference for the government's inquiry. Historians in the future (including the not very distant future) will wish to explore what consideration Whitehall gave to the problems it is now confronting.

The terms of reference for the Butler report, nevertheless, enabled a broader assessment of the role of British intelligence in countering the proliferation of weapons of mass destruction. A central conclusion was that failure over Iraq should be set against four intelligence successes (Iran, North Korea, Libya, and the private network of Mr A. Q. Khan). The problems of counterproliferation and counterterrorism have not gone away with the fall of Saddam Hussein. It remains to be seen how far humanitarian intervention (as in Kosovo) or preventive counterproliferation (as in Iraq) represent precedents or watersheds. It nevertheless seems reasonable to conclude that changes in international politics will make the public use of intelligence much more common practice. The emergence of "pre-emptive self-defense" in the United States has introduced an important new dimension to the role of intelligence in international relations. Public (and parliamentary) opinion will need much more convincing in order to support preemptive interventions, although British public opinion is likely to remain hostile to any military adventures. Intelligence is clearly central to this, and pressure will surely increase on governments to disclose the secret intelligence on which they base their actions.

THE STUDY OF INTELLIGENCE IN BRITAIN

A recent survey of academic teaching in intelligence studies identified over thirty scholars teaching intelligence in British universities.[68] Undergraduate and Taught Master's courses are to be found in departments/schools of international politics, international history, history, politics, and war studies. The survey also notes the growing interest and concern among lawyers where growing conflicts between human rights and human security are apparent. Academic papers on intelligence and intelligence-related subjects are a normal part of the annual conferences of the British International History Group, the British International Studies Association, and the British Political Studies Association, which since 1993 hosts it own Security and Intelligence Studies Group. And there are now two dedicated centers for the study of intelligence (at Brunel and Aberystwyth). The study of intelligence is now embedded in British universities, and from differing methodological and critical perspectives. These differing perspectives are reinforced by authoritative works by journalists and other writers, some of whom have explored areas that British intelligence scholars have been reluctant to engage, such as Northern Ireland.[69]

The scale of British endeavors is nevertheless dwarfed by those in the United States, where the openness of the intelligence process has furthered the cause of policy-relevance inquiry. The idea of speaking truth unto power has clear relevance to the relationship between government and academia. In the United States there has been a significant relationship between scholars and officialdom, and the CIA has actively promoted the teaching and academic study of the subject. Both the National Security Agency and the CIA each employ their own team of full-time professionally trained historians and have invited "scholars in residence" to spend extended periods working within the agencies.

In Britain no such relationship exists. A greater distance has been maintained between academics and practitioners. There have been important exceptions to this general trend, most notably the scholars who were given privileged access to archives to write the official histories of World War II. But only recently has a culture of greater openness begun to foster greater engagement between Britain's intelligence community and its universities. Illustrative of this trend was the willingness of Sir Stephen Lander, then director-general of MI5 (and a Cambridge-trained historian), to attend academic meetings and conferences on the study of intelligence.[70] Further evidence of engagement was the appointment of academic historians to write the centenary histories of MI5 and SIS. There are those who argue that engagement is not without costs, and that in the words of one intelligence historian "official histories of this kind belongs to the era of deference to government and fits awkwardly with a modern intelligence service"—a better approach would be to make the records available to all historians.[71] The recent establishment of an Advisory Group on Security and Intelligence Records in July 2004 under the Cabinet Office with academic representation may be a positive move.[72] However, on present trends it could be

a decade or more before records of MI5 and GCHQ are available to post-1945 Cold War, postcolonial, and other historians (and a century or two before those of SIS reach the National Archives). Nevertheless, the relationship between academics and practitioners shows signs of change and one manifestation of this is that some scholars are becoming more willing to provide policy-relevant prescriptions.[73]

CRISIS AND OPPORTUNITY

In 2003 Britain supported the American war on Iraq, in part because of mistaken intelligence assessments about Iraqi weapons of mass destruction. Has this created a crisis of confidence in British intelligence? Or do the problems of disclosing intelligence on Iraq augur a reassessment of greater openness and a retreat from the advances of recent years? What are the implications for those who study the subject? To talk of crisis is surely exaggeration. Those who were critical or hostile to intelligence before Iraq have been reinforced in their views. The credibility of British intelligence has been damaged, notwithstanding the attempts of the Butler report to place the failure in the context of four other successes. What is now unprecedented in Britain is for senior security and intelligence officials to make clear that it is only a matter of time before British cities are attacked with "unconventional" weapons such as radiological or biological weapons. When—or if—that happens, the term "crisis" may well be more readily applied.

At the time of writing the prospect of confrontation with Iran looms large while discussion of military confrontation exists at the margins. Mobilizing domestic or international opinion to support action against Tehran has been made significantly harder by what occurred over Iraq. The manner in which intelligence was used on Iraq reflected the style of the Blair government and its approach to public and media relations. Tony Blair will soon cease to be prime minister. Moreover, one very clear lesson from Iraq was that the efforts of United Nations Special Commission (UNSCOM) and the International Atomic Energy Authority (IAEA) were underestimated in identifying and dealing with the situation in Iraq from 1991 to 1998. The IAEA has played a crucial role in taking forward concern about Iran's behavior. Skepticism about British intelligence has not extended to the IAEA. Nevertheless, the public justification of action that is based on intelligence assessments will require much further thought than happened over Iraq.

The professional and public responsibility of academics who study intelligence is to foster greater understanding of the nature and role of intelligence, including not only its value but its limitations. These include understanding the limitations of our knowledge of what is done in secrecy by our governments. It is a small act of optimism to suggest that, notwithstanding recent difficulties, the momentum for greater disclosure and accountability will continue, though it may well be that advances in open government including freedom of information

legislation may have deleterious unintended consequences. One aspect of the recent inquiries into the Iraqi intelligence failure is that internal communications (including e-mail) were brought into the public domain. There is reason to believe that officials may now be much more careful about what they commit to permanent record and much more eager to destroy it when they have.[74] Nevertheless, the opportunities for studying intelligence in Britain, and the opportunities to study them by means of differing methodological and theoretical approaches, have never been more propitious. There are some advantages to living in interesting times.

NOTES

Themes in this chapter are developed from a research project on intelligence methodology conducted by myself and Peter Jackson, funded by the British Academy and the University of Wales, Aberystwyth; see L. V. Scott and Peter Jackson, "Journeys in Shadows," in *Understanding Intelligence in the Twenty-first Century: Journeys in Shadows* (London: Routledge, 2004), pp. 1–28, and Peter Jackson and Len Scott, "Intelligence," in Patrick Finney, ed., *Palgrave Advances in International History* (Basingstoke: Palgrave/Macmillan 2005), pp. 161–88. I am very grateful to the following for their comments on earlier drafts of this chapter: Richard Aldrich, R. Gerald Hughes, Peter Jackson, and Stephen Twigge.

1. See Matthew M. Aid, ed., "Declassification in Reverse: The Pentagon and the U.S. Intelligence Community's Secret Historical Document Reclassification Program," available at the National Security Archive website: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB179/.

2. See, for example, Robert A. Goldberg, "Who Profited from the Crime? Intelligence Failure, Conspiracy Theories, and the Case of September 11," in L. V. Scott and Peter Jackson, *Understanding Intelligence in the Twenty-first Century: Journeys in Shadows* (London: Routledge, 2004), pp. 99–110.

3. For a historical overview, see Peter Jackson, "Historical Reflections on the Uses and Limits of Intelligence," in Peter Jackson and Jennifer Siegel, eds., *Intelligence and Statecraft: The Uses and Limits of Intelligence in International Society* (London: Praeger, 2005), pp. 11–51.

4. For overviews of official British attitudes toward secrecy, see K. G. Robertson, *Secrecy and Open Government: Why Governments Want You to Know* (London: Macmillan, 1999); David Vincent: *The Culture of Secrecy: Britain, 1832–1998* (Oxford: Oxford University Press, 1998); and Richard Thurlow, *Secret State: British Internal Security in the Twentieth Century* (Oxford: Blackwell, 1994).

5. House of Commons, *Official Record,* 15 December 1924, col. 674.

6. J. C. Masterman, *The Double-Cross System in the War of 1939 to 1945* (New Haven and London: Yale University Press, 1972).

7. F. W. Winterbotham, *The Ultra Secret* (London: Weidenfeld and Nicolson, 1974).

8. Nigel West, "Fiction, Faction and Intelligence," in Scott and Jackson, *Understanding Intelligence*, p. 123.

9. Peter Wright, *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer* (New York: Viking, 1987).

10. See Philip Knightley, *The Second Oldest Profession: The Spy as Patriot, Bureaucrat, Fantasist and Whore* (London: Pan, 1987), and James Rusbridger, *The Intelligence Game: The Illusions and Delusions of International Espionage* (London: The Bodley Head, 1989).

11. Christopher Andrew, "Historical Research on the British Intelligence Community," in Roy Godson, *Comparing Foreign Intelligence: The U.S., the USSR, the U.K. and the Third World* (London: Pergamon-Brassey's, 1988), pp. 52, 54.

12. House of Commons, *Official Record,* 6 May 1992, col. 65. Former Prime Minister Callaghan wrote of his dealings with the chief of SIS in his 1987 autobiography, James Callaghan, *Time and Chance* (London: Collins, 1987), p. 375.

13. Gill Bennett, "Declassification and Release Policies of the U.K.'s Intelligence Agencies," in Oliver Hoare, ed., *British Intelligence in the Twentieth Century: A Missing Dimension?, Intelligence and National Security*, 17 (Spring 2002), p. 24, special issue.

14. Peter Gill, "Reasserting Control: Recent Changes in the Oversight of the U.K. Intelligence Community," *Intelligence and National Security*, 11 (April 1996), p. 327.

15. On ECHELON, see: http://cryptome.org/echelon-ep-fin.htm; on CIA detention centers, see: http://www.europarl.eu.int/news/public/story_page/015-5903-065-03-10-902-20060308STO05902-2006-06-03-2006/default_en.htm.

16. http://www.nationalarchives.gov.uk/recordsmanagement/selection/pdf/osp8.pdf; http://www.nationalarchives.gov.uk/recordsmanagement/selection/pdf/osp28.pdf. I am grateful to Stephen Twigge for drawing my attention to these.

17. Christopher Andrew and David Dilks, eds., *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century* (Urbana: University of Illinois Press, 1984).

18. For an authoritative overview, see Richard Aldrich, "Policing the Past: Official History, Secrecy and British Intelligence since 1945," *English Historical Review,* 119 (September 2004), pp. 922–53.

19. Sir Michael Howard, *British Intelligence in the Second World War Volume 5: Strategic Deception* (London: H.M. Stationary Office, 1990).

20. Quoted in Knightley, *Second Oldest Profession*, p. 111.

21. Richard Aldrich, " 'Grow Your Own': Cold War Intelligence and History Supermarkets," in Hoare, *British Intelligence,*pp. 145–6.

22. http://www.mi6.gov.uk/output/Page5.html.

23. Sir Lawrence Freedman, *The Official History of the Falklands Campaign Vol. 1: The Origins of the Falklands War* (London: H.M. Stationary Office, 2005); *Vol. II War and Diplomacy* (London: H.M. Stationary Office, 2005).

24. G. Bennett and K. A. Hamilton, *Documents on British Policy Overseas Series III Vol 1 Britain and the Soviet Union, 1968–72* (London: Stationary Office, 1997).

25. Gill Bennett, *"A Most Extraordinary and Mysterious Business": The Zinoviev Letter of 1924* (London: FCO, 1999).

26. Gordon Brook-Shepherd, *Iron Maze: The Western Secret Services and the Bolsheviks* (Basingstoke: Macmillan, 1998).

27. Andrew Cook, *On His Majesty's Secret Service: Sidney Reilly ST1* (Stroud, U.K.: Tempus, 2002).

28. Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (London: Hodder and Stoughton, 1990).

29. Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West* (London: Allen Lane, 1999).

30. Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive II: The KGB and the World* (London: Allen Lane, 2005).

31. Andrew and Dilkes, *The Missing Dimension,*p. 5.

32. David E. Murphy, Sergei A. Kondrashev, and George Bailey, *Battleground Berlin: CIA vs KGB in the Cold War* (New Haven, CT: Yale University Press, 1997), pp. 449–53.

33. Nigel West and Oleg Tsarev, *The Crown Jewels: The British Secrets Exposed by the KGB Archives* (London: HarperCollins, 1999), pp. 279–345.

34. See, in particular, Paul Maddrell, *Spying on Science: Western Intelligence in Divided Germany 1945–61* (Oxford: Oxford University Press, 2006).

35. Bennett, "Declassification and Release," p. 28.

36. See the CIA's website: http://www.foia.cia.gov/penkovsky.asp These and other documents were made available to facilitate an account of the espionage of Oleg Penkovsky by Jerrold Schecter and Peter Deriabin: *The Spy Who Saved the World: How a Soviet Colonel Changed the Course of the Cold War* (New York: Charles Scribner's Sons, 1992).

37. Wesley K. Wark, "In Never-Never Land? The British Archives on Intelligence," *The Historical Journal*, 35 (1992), pp. 198–9.

38. Richard Aldrich, *The Hidden Hand: Britain, America and Cold War Secret Intelligence* (London: John Murray, 2001), p. 5.

39. See, for example, Andrew Defty, *Britain, America and Anti-Communist Propaganda, 1945–1958: The Information Research Department* (London: Frank Cass, 2004), and James Vaughan, " 'Cloak Without Dagger': How the Information Research Department Fought Britain's Cold War in the Middle East, 1948–56," *Cold War History* 4 (April 2004), pp. 56–84.

40. See Philip H. J. Davies, "From Special Operations to Special Political Action: The 'Rump SOE' and SIS Post-War Covert Action Capability 1945–1977," *Intelligence and National Security* 15 (2000). For accounts of operations, see Aldrich, *Hidden Hand*; Mark Urban, *U.K. Eyes Alpha: The Inside Story of British Intelligence* (London: Faber and Faber, 1996); and Stephen Dorril, *MI6: Fifty Years of Special Operations* (London: Fourth Estate, 2000).

41. For accounts of operations and planning in the Middle East, see Tom Bower, *The Perfect English Spy, Sir Dick White and the Secret War 1935-90* (London: Heinemann, 1995), pp. 185–224; Aldrich, *Hidden Hand*, pp. 464–93, 581–606; and Dorril, *MI6*, pp. 531–699.

42. For discussion, see Philip H. J. Davies, *MI6 and the Machinery of Spying* (London: Frank Cass, 2004), pp. 297–8.

43. Urban, *U.K. Eyes Alpha*, pp. 34–7.

44. Peter Taylor, *The Provos: The IRA and Sinn Fein* (London: Bloomsbury, 1997), pp. 129–47, and *Brits: The War Against the IRA* (London: Bloomsbury, 2001), p. 80 et seq; see also Len Scott, "Secret Intelligence, Covert Action, and Clandestine Diplomacy," in Scott and Jackson, *Understanding Intelligence*, pp. 173–5.

45. Richard Tomlinson, *The Big Breach: From Top Secret to Maximum Security* (Edinburgh: Cutting Edge Press, 2001), p. 73.

46. Tomlinson, *The Big Breach,* pp. 106–7, 140, 179–96.

47. The document can be found at: http://www.cryptome.org/qadahfi-plot.htm.

48. Dorril, *MI6*, p. xiv.

49. Scott A. Koch, *"Zendebad, Shah!": The Central Intelligence Agency and the Fall of Iranian Prime Minister Mohammed Mossadeq, August 1953* (Washington: CIA History Staff, 1998).

50. C. M. Woodhouse, *Something Ventured* (London: Granada, 1982).

51. Donald Wilber, *CIA Clandestine History, Overthrow of Premier Mossadeq of Iran, November 1952–August 1953*, available at the National Security Archive website: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB28/index.html.

52. *New York Times* website: http://www.nytimes.com/library/world/mideast/iran-cia-intro.pdf; National Security Archive website: ibid.

53. "American President 'Ordered African Killing,' " *Guardian*, 10 August 2000; "Eisenhower Ordered Congo Killing," *Independent*, 14 August 2000.

54. Matthew Jones, "The 'Preferred Plan': The Anglo-American Working Group Report on Covert Action in Syria, 1957," *Intelligence and National Security* 19 (Autumn, 2004). The key archival sources are in the private papers of Duncan Sandys.

55. Freedman, *Official History Vol. 1*, pp. 85–8; James Callaghan, *Time and Chance* (London: Collins, 1987), p. 375.

56. Lord Franks, et al., *Falkland Island Review: Report of a Committee of Privy Counsellors,* Cmnd 8787 (London: HMSO, 1983), paras 64–6, 327, pp. 18–19, 87.

57. Freedman, *Official History*; David Owen, *Time to Declare* (London: Michael Joseph, 1991), p. 350.

58. Peter Hennessy, *The Secret State: Whitehall and the Cold War* (London: Allen Lane Penguin Press, 2002), p. xiii.

59. Michael Herman, "Modern Intelligence Services: Have They a Place in Ethical Foreign Policies?" in Harold Shukman, ed., *Agents for Change: Intelligence Services in the 21st Century* (London: St. Ermin's Press, 2000), pp. 287–328.

60. See Toni Erskine, " 'As Rays of Light to the Human Soul'? Moral Agents and Intelligence Gathering," in Scott and Jackson, *Understanding Intelligence*, pp. 195–215; and Sir Michael Quinlan, "Ethics and Intelligence," second annual lecture of the Centre for Intelligence and International Security Studies, November 2005, *Intelligence and National Security*, forthcoming.

61. See, in particular, Davies, *MI6 and the Machinery of Government*.

62. Lord Butler, et al., *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Counsellors*, HC 898 (London: H.M. Stationary Office, July 2004).

63. House of Commons Select Committee on Foreign Affairs, *The Decision to Go to War with Iraq*, ninth report of the session 2002-3, HC 813-I, vol.1, 3 July 2003; Intelligence and Security Committee, *Iraq Weapons of Mass Destruction—Intelligence and Assessment*, Cm 5972, 9 September 2003; Lord Hutton, *Report of the Inquiry into the Circumstances Surrounding the Death of Dr. David Kelly*, available at http://www.the-hutton-inquiry.org.uk/; Butler, *Review of Intelligence.* For discussion, see Richard Aldrich, "Whitehall and the Iraq War: The U.K.'s Four Intelligence Enquiries," *Irish Studies in International Affairs* 16 (2005); Alex Danchev, "The Reckoning: Official Enquiries and the Iraq War," *Intelligence and National Security* 19 (Autumn, 2004); and Anthony Glees and Philip H. J. Davies, *Spinning the Spies: Intelligence, Open Government and the Hutton Inquiry* (London: Social Affairs Unit, 2004).

64. Scott and Jackson, "Journeys in Shadows," and Peter Jackson and Len Scott, "Intelligence," in Patrick Finney, ed., *Palgrave Advances in International History* (New York: Palgrave /Macmillan 2005), pp. 161–88.

65. Andrew Rathmell, "Towards Postmodern Intelligence," *Intelligence and National Security* 17 (2002), pp. 87–104.

66. For constructivist approaches to IR, see, for example, the essays in Peter J. Katzenstein, ed., *The Culture of National Security* (New York: Columbia University Press, 1996), and Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999).

67. Christopher Andrew, "Intelligence, International Relations and 'Under-theorization,' " in Scott and Jackson, *Understanding Intelligence*, pp. 29–30.

68. Paul Maddrell, "Intelligence Studies at U.K. Universities," Autumn 2003, available from the CIISS at: http://www.aber.ac.uk/interpol/research/CI.html.

69. Mark Urban, *Big Boys' Rules: The SAS and the Secret Struggle Against the IRA* (London: Faber and Faber, 1992); Taylor, *Brits*; Tony Geraghty, *The Irish War: The Hidden Conflict Between the IRA and British Intelligence* (Baltimore: Johns Hopkins, 2000).

70. See, for example, the inaugural lecture of the CIISS at Aberystwyth, given by Sir Stephen Lander in November 2004 and published in *Intelligence and National Security*, forthcoming.

71. E.D.R. Harrison, Letter to *The Times*, 15 August 2002.

72. http://www.cabinetoffice.gov.uk/about_the_cabinet_office/other_bodies/horuintel.asp. I am grateful to Stephen Twigge for drawing my attention to this.

73. See, for example, Glees and Davies, *Spinning the Spies.*

74. Aldrich, "Whitehall," p. 83. Aldrich notes the emerging phenomenon among civil servants of "shredding day" to dispose of potentially compromising material.

6

SEARCHING WHERE THE LIGHT SHINES?

An American View of Methods for the Study of Intelligence

MICHAEL WARNER

REFLECTIONS ON AN "AMERICAN VIEW" OF STUDYING intelligence should not be confused with any particularly "American method" for doing so. Indeed, there is no distinctly American form of intelligence. The craft of intelligence work has been performed according to its own seemingly immutable principles since ancient times, wherever sovereign powers have fought each other or remained ready to do so. The deadly realities of interdynastic (even if not quite international) conflict have always made rulers and commanders desire to keep and steal secrets, and to employ the clandestine arts to strengthen their friends and weaken their adversaries.

Nonetheless, there are American "idioms" for the practice of intelligence. It emerged as a professional discipline in the United States during and after World War I, developing from three prior disciplines: diplomacy, reconnaissance, and law enforcement. The dividing lines between it and these fields have remained ambiguous, and porous. At least since World War II, intelligence in the United States has been conducted in ways that are comparatively large-scale, expensive, technological, and ad hoc. Intelligence in America tends to be pragmatic, in crafting solutions and then only later examining them for principles that made them work. American intelligence also tends to be comparatively visible, in that many of its secrets do not remain hidden for long, whether from institutional or political rivals, congressional and media monitors, and ultimately the public.

The study of intelligence in America has proceeded on similar lines. The United States came late to the professional practice of intelligence, but researchers in America developed the study of intelligence at least as fast as scholars in other nations. The scholar of it must know something of both war and diplomacy—particularly how states defend themselves and employ their "levers of national

power"—to understand intelligence. Historical scholarship on this topic in the United States has been based on two trends: on the episodic employment of official historians (and the later release of their studies), and on the investigative declassification (often driven by political motivations) of reports, documents, and sometimes files relating to certain controversial episodes. If there is anything like an American method of studying intelligence, it would represent the collectivity of the particular methods employed in using those resources. It would thus also be influenced, at least indirectly, by the source materials that have been made available.

What follows is not a bibliographical or archival guide to records holdings in the United States. It is not possible in one article to survey the collections of the National Archives and the holdings of the agencies of the U.S. Intelligence Community. Even for researchers such a survey would have the ironic disadvantages of being both too detailed and too vague. It would also be quickly out of date as new files are released. This chapter is rather a reflection on the types of sources that are available and, more important, on the ways in which they influence the methods employed by scholars of American intelligence.

INTELLIGENCE AND SCHOLARSHIP

Intelligence can be thought of as that which states do in secret to support their efforts to mitigate, influence, or merely understand other nations (or at least their enemies). By its nature as an activity that risks the loss of fragile sources of information or other means of understanding and influence—and that can affect the lives of troops, subjects, and even leaders—intelligence is treated by its practitioners as sensitive and confidential. Even the accidental disclosure of some analytical, informational, or operational advantage over a rival is presumed to be tantamount to the loss of that advantage while it is still potentially useful. Thus the penalties for disclosure have always been severe (and those for espionage even harsher). Wherever such life-and-death stakes obtain—and the United States is no exception—intelligence is done with some full or partial cloak of secrecy, and the documentary record of it is typically unavailable to onlookers.

Intelligence thus, by definition, resists scholarship, but in the United States there are countervailing forces in the nation's culture and polity that have mitigated the secrecy that customarily surrounds the discipline. First, Americans seem almost congenitally predisposed to distrust government in general and secret dealings in particular. Second, the nation's citizens and institutions practically relish holding officials accountable for their stewardship of the public's trust and resources; this phenomenon is magnified by large news and popular media industries competing for scoops and gripping tales for retail sale. The nation's two-party polity, furthermore, breeds mutual suspicion of anything resembling partisan or ideological interference with public institutions. Finally, the Constitution's implicit endorsement of strong executive branch departments (and its

comparative silence on the means to coordinate their efforts) fosters an institutional culture of independence and self-subsistence among the Cabinet-level departments, with each seeking to provide for its own needs in a variety of fields, including intelligence (not infrequently in duplicative ways).

These antisecrecy trends and inclinations sometimes interact to convince administrations, Congresses, and intelligence agency heads that they must release various historical intelligence documents. Even when such decisions are taken, however, the compartmented organization of the executive branch usually ensures that declassification proceeds on a piecemeal, agency-by-agency basis—instead of being undertaken in a way that illuminates the workings of the entire intelligence system.

Scholarship has trended accordingly. Over the last sixty years, scholars in the employ of the U.S. government have episodically sought to understand the experiences of the nation's intelligence services. Various Cabinet departments and intelligence agencies have hired professional historians, or appointed chroniclers from their own ranks, to write narratives of their recent activities. The Office of Strategic Services (OSS), for instance, gave this job to operative Kermit Roosevelt after World War II; the fledgling Central Intelligence Agency (CIA) lured Arthur Darling from Yale; and the Armed Forces Security Agency tapped the U.S. Navy's Commander Laurance Safford.[1] In addition, the armed services' histories of their efforts in World War II—most notably the U.S. Army's "Green" series, but also the less-ambitious though still-substantial efforts by the other services—discussed intelligence matters as well at greater or lesser length. This tradition of ad hoc, in-house scholarship has endured to the present day, and over the last generation it has been supplemented by more strongly professional and institutionalized efforts in the Intelligence Community, the military, and the State Department (via the *Foreign Relations of the United States* series). The results of all these efforts have been uneven, but they have been real, and in places they have laid a solid foundation of fact that can support serious theoretical inquiry.

The federal government has not been content with allowing cleared official historians to read its intelligence records. The United States, having performed little clandestine work overseas before 1941, has been comparatively liberal in opening up the files of actual intelligence offices up to around the middle of the 20th century. The best such pre–Cold War collection is that of the OSS, which Director of Central Intelligence William J. Casey had declassified in the 1980s. That process took several years longer than Casey might have anticipated, but now virtually all OSS files are available at the National Archives, and the rather haphazard collection (reflecting OSS's chaotic administrative practices) has been given an improved set of finding aids. The OSS files were and are important in themselves, being the first nearly complete records of the birth, maturity, and demise of a modern intelligence agency (from a nation that had not been conquered and occupied) to be made available to scholars. OSS was a sprawling agency, moreover, practicing several intelligence disciplines and engaging in

hundreds of individual operations, and thus a researcher can read in its files documents on a wide variety of activities.

The release of OSS files has been accompanied by the broad declassification of diplomatic, military, and internal security files up to the mid-20th century. Most records of the State, War, and Navy Departments up to that point and sometimes beyond are now available, including their intelligence files (except where those identify foreign sources or cryptologic methods). Many files of the Federal Bureau of Investigation (FBI) from before the Cold War have been declassified as well, though case files on individuals are available (if at all) through Freedom of Information Act requests. The holdings of the Franklin D. Roosevelt presidential library are virtually all available, whereas the Harry S Truman Library holds only a dwindling set of files in classified storage.

The net effect of these releases has been to make it possible for academic and private researchers to see all but a few of the extant documents on American intelligence up to 1946, and many of those documents for several years thereafter. In dealing with intact files, like those of OSS and other agencies, researchers use methodologies that are quite similar to those employed by official historians doing research in still-classified records. Both the "inside" and the "outside" historians work primarily from the office and operational files, from cable traffic and budget data, and from interviews (where living memory endures), artifacts, and other sources, to identify and assemble the clues to what happened and what it meant. The result can be a detailed and insightful appraisal of U.S. intelligence capabilities and performance, such as Katherine Sibley's *Red Spies in America*, on Soviet industrial espionage in the 1940s.[2]

The first place for the researcher to look is always "the file." Like virtually all governmental organizations from the late 19th century onward, intelligence agencies are hierarchies, and their officers at multiple levels have created and preserved files on their activities. Just as the sources for intelligence history are often the same as those used by military and diplomatic historians, the methods for using them are similar as well. The sort of the files that get saved at the State Department or one of its military counterparts—and eventually made available to historians—tend to be archived by office first, by subject next, and then sometimes by operation or activity, according to the records protocols governing the larger department or organization in which they are embedded. The independent intelligence agencies of the United States adapted their filing schemes from the State and War Departments (with minor adjustments to fit their specific needs). The FBI adopted its filing system from the Department of Justice.

The more expensive the activity or topic, the more places one finds files on it. Costly activities and projects ordinarily require more personnel and logistical expenses, hence more accounting and security controls—and more legal counsel—and thus more files. An agency's legal, financial, logistical, and security offices can be expected to keep their own files on larger activities. The director of the agency may have a file on it, if it demands his attention or a briefing for higher authorities. Something really important will merit files in other agencies, and in

the presidential libraries as well. These can be quite valuable for the researcher because they provide a different (if not always more objective) perspective on the activity.

Not all important incidents, projects, issues, or events are well documented. Here is a quandary in intelligence research: what to infer from a situation in which there are few or no files. That can happen in two circumstances. The first is when events are happening too quickly for everything to be documented by the people on the spot. In such cases the documentation will typically come in the form of summary cables and after-action reports, which are not always as accurate and complete as a researcher might wish. The second case is when the head of the agency or one of its units is specifically ordered to keep the "paper trail" as short as possible. Such instances are rare, but the exceptions that prove the rule (like the CIA's "Track II" in Chile in 1970) are notorious.[3] One reason there were not more such exceptions, even at the height of the Cold War, is the difficulty of doing anything of consequence in a bureaucracy without written authorizations and regular funding streams. When an exception is made, typically some extraordinary aspect will be added to an operation already under way, as with the abortive assassination plotting in the CIA's Guatemala coup operation in 1954.[4] Such operational annexes would usually have been authorized orally.

The next place to look for records, especially if the activity took place overseas, is in the cable traffic. Intelligence agencies live by their official communications channels, and the messages routed along them are meticulously preserved and organized. Cables are supposed to be terse and clear, for the safety and success of the operation and the people involved, not to mention the expense of sending them. Indeed, when compared with staff memoranda produced at a comparatively leisurely pace in the home offices, cables generally seem both laconic and articulate. Cables could take many hours to reach their recipients, however, and not a few cabled instructions had been overtaken by events by the time their addressee finally read them.

Files and cables, where available, allow the researcher to establish accurate chronologies. Where chronology is not, or cannot be, established, the conclusions drawn from the evidence must be regarded as tentative or even as suspect. Chronology is a vital clue in sorting causes and effects, and more than one "urban legend" circulated among intelligence officials (and even among scholars) has been debunked by the simple method of carefully charting events along a reliable time sequence.

A third key source for researchers is budget data. Budgets are sure indicators of the priorities of an organization, and of that organization's priority in the larger scheme of policy implementation. They are also an index for comparison in looking at operations themselves, indicating as they do the relative size of the operation in relation to other activities. Agencywide budgets serve another purpose—that of giving the researcher a benchmark for the quality and challenges of leadership. Declining budgets are a severe test of a leader's ability. On the one hand, tough decisions are forced on a leader in such times; he or she has to trim

somewhere to preserve other priorities, and such choices generally result in disagreements and even bitterness among the managers whose projects and offices lose out. On the other hand, growing budgets allow him or her to throw money at problems, and many directors are tempted to do just that, often with meager and short-lived results.

Another help, sometimes, is the personnel file of someone involved in an activity. If it contains performance evaluations for the time in question, or names of other people involved, such a file gives a researcher important reference points. It also provides clues to the orientation of the officer in question—his professional training and background—that may have had a bearing on the decisions or operation in question. Knowledge of the personnel involved also helps in surmounting the difficulties posed for intelligence scholarship that are caused by secrecy and compartmentation. One cannot assume that an event that was prior in time helped to cause a later one, or that a prior report caused a subsequent decision, since the personnel involved may have had no access to such information. Sometimes it is possible to show that someone involved in an earlier operation was in a position to have had a role in a later one. The converse is true as well—sometimes two things that looked similar were really independent, with no common personnel.

This discussion of sources for official research in intelligence must seem quite elementary to any historian working in the documentary record of 20th century military or diplomatic history. That is no coincidence, for military and diplomatic history is precisely what historical research in intelligence is. Intelligence is not some privileged realm where the usual rules of organizational dynamics and group behavior do not apply; thus it is no exception to the rules of historical scholarship. One gathers the records and facts and arranges them according to the time-honored ways of archival practice and scholarship. An intelligence service will possess more secrets, and sometimes more colorful characters, but its job is to assist the making and the implementing of a nation's strategic decisions. Its records therefore exist in the same milieu and the same patterns as the diplomatic and military ministries that intelligence serves.

METHODS FOR THE COLD WAR AND BEYOND

Though our knowledge of U.S. intelligence before the 1950s is fairly good, many researchers in American intelligence history are interested in the period of the Cold War and its aftermath. For them, the sources are typically piecemeal and incomplete. Many of the records sent to the National Archives after 1950 represent "finished" intelligence products—i.e., disseminated intelligence analysis. Few policy or administrative documents, and even fewer operational records, have been released. Complete files are rarer still. The spotty official documentation available to academic and private researchers makes their task difficult, though not impossible.

These researchers' works on American intelligence are in some ways more interesting than the official histories because their authors faced a more difficult task. Where few records have been released, the researcher has to appraise his or her sources in the knowledge that they are surely fragmentary. He has to word his judgments accordingly, erring always on the side of caution, and building to generalizations only on stable bases of fact. Intelligence studies in academia have nevertheless quickened over the last three decades in the fields of history and political science, as more scholars of the diplomatic and military arts grasp the importance of intelligence for their own disciplines, and gain familiarity with the relevant documentation. The methods of these "outside" scholars can, in skilled hands, bring their practitioners to genuine historical understanding.

Writing about intelligence in the absence of hard archival sources is a labor that strongly resembles the writing of ancient history. Much of the best writing in this genre is heavily literary in character, rather than historical in the Rankean sense of depicting events "wie es eigntlich gewesen war" [as they actually happened]. This is not meant as a criticism or a pejorative. Livy, Tacitus, and Thucydides, to name three classical scribes, sought by the portrayal of fascinating but flawed characters against the backdrop of grand narratives to illustrate the larger themes of nature, society, and man himself.[5] The intelligence histories that have been written along different but not dissimilar lines tend to be entertaining and insightful about the characters that populate their narratives.

Where histories of American intelligence aspire to be more Rankean than literary, they tend to resemble in some ways the works of modern historians writing about ancient times. They have to rely on fragments, not files. Their chronologies are sometimes hazy. Rumor and myth are everywhere, often so intertwined with fact that, in some cases just beyond the reach of living memory, truth and fiction can no longer be separated. The one obvious advantage that intelligence historians have over ancient historians is in the opportunity to interview their subjects—when they will talk (which is sometimes at considerable length). Acquiring the real documents, when one does not have the files they came from, is only the beginning of the task for academic and private researchers. It can be tricky to match them up with the accreted legends that both informed and were themselves formed by an earlier body of literature written without any access to the sources (historians of ancient Greece have a similar chore in squaring the tangible discoveries of modern archeology with the epics of Homer, for instance).

A careful nonofficial researcher tracks down any official documents, studies, reports, and histories that might be available on his or her topic. Congressional testimony and floor debates, and (in recent years) the committee reports accompanying the annual Intelligence Authorization Acts, are particularly good sources. The Central Intelligence Agency (where this author once worked) has released several dozen monographs and compilations on its history, and the National Security Agency's release efforts are equally extensive. The armed service intelligence offices have done their share of publishing as well. Such

official releases have their distinct limitations. Especially when written by long-serving agency officers (as opposed to professional historians), they typically display a lack of methodological ambition, being straightforward, chronological organizational or operational narratives. They are straitened by the scope of their charters, by the rigors of the declassification process, and by the aptitudes and curiosity of their authors. Nonetheless, they provide an important touchstone of accepted fact that the researcher can use as a platform for further inquiry, or at least a landmark along the way.

The reports of blue-ribbon study commissions and investigative panels can also be illuminating, and even crucial to the researcher's work. A watershed for scholars of the U.S. Intelligence Community came with Congress's publication of the *Final Report* of the Senate's special committee that met under the leadership of Senator Frank Church (D-Idaho) in 1975–76. It is no exaggeration to say the "Church Committee's" seven volumes laid the foundation for public knowledge of American intelligence. The committee's survey of the history of the Central Intelligence Agency from its founding to the mid-1970s is particularly valuable, in being comprehensive, insightful, and reliable (in large part because it was based on several dozen still-classified histories produced or held in the CIA's history staff).[6] There are also examples of official inquiries that made it to the public via extralegal routes, like the Department of Defense's historical compilation relating to the Vietnam War (the "Pentagon Papers," 1971) and the House of Representative's select committee on intelligence report that was rejected by the full House in 1976 (the "Pike Report").[7]

The researcher next looks for the declassified documents themselves. In some cases, the government has released extensive records on particular controversial incidents or topics. Although several of these large-scale declassifications were undertaken for the purpose of clearing the air on certain topics, others were related to congressional investigations or even criminal prosecutions; in both of these latter cases there were political or legal motivations (and sometimes both) for releasing the material. The releases themselves range from the work done by U.S. authorities to track (and occasionally exploit) Nazis and the assets they looted in World War II, to the recent flap over the intelligence on Saddam Hussein's weapons of mass destruction. Other examples include the early Cold War effort to read Soviet intelligence communications and capture Russian agents (VENONA); efforts to destabilize the governments of Guatemala (1954), Cuba (1959–64), Chile (1970–73), and Nicaragua (1983–86); intelligence on the assassination of President Kennedy; and analysis and operations related to Al Qaeda before the attacks of September 11, 2001. It should be noted that these releases also have the larger, penumbral effect of setting precedents that encourage the subsequent release of other and related materials as well.

The timing of these releases is a critical factor in judging the reliability of scholarly work on U.S. intelligence. Knowing not only the sequence of intelligence activities and events but also the timing of the production and subsequent release of (both internal and public) information about them helps one judge the

value of secondary reference materials (and even of some primary sources). It is crucial to understand how much material was and was not available to the author of a history or the drafter of a memo. Anything written about intelligence against Germany in World War II, for instance, must be read with particular care if it was published before the revelation of the ULTRA secret in 1974. Similarly with works on certain Cold War espionage cases in the United States, if published before the public release in 1995 of the VENONA cables (the decryptions of Soviet intelligence telegrams sent to and from foreign posts, mostly during World War II). It is even a factor to consider when reading histories written by government historians. Several early official histories of U.S. intelligence, for example, were written without access to the mysteries of signals intelligence or the outlines of important human intelligence operations. This reality does not falsify the arguments or discredit the facts cited in works published before these key releases, but it does make them incomplete in important ways.

Much documentation continues to come out through official responses to private requests for documents. The main avenue for such releases has been the Freedom of Information Act (often referred to by its acronym, FOIA). Although not unreasonably scorned by some researchers and declassification advocates as hopelessly slow and haphazard, FOIA requests have nonetheless cumulatively resulted in the release of millions of pages. A requester needs to describe what he or she wants with a fair degree of precision, and then to be very patient, but such virtues are sometimes rewarded. Peter Grose's *Operation Rollback* on early CIA covert action programs, and Kathryn S. Olmsted's *Red Spy Queen* on Soviet spy-turned-informant Elizabeth Bentley, are two recent examples of important works based largely on documentation obtained through FOIA requests.[8]

A handful of researchers have availed themselves of Section 4.4 of Executive Order 13292 (and its predecessors), which allows agency heads to grant scholars engaged in meritorious "historical research projects" limited access to still-classified files. Evan Thomas's *The Very Best Men* is an example of what can be accomplished via this route; Benjamin Weiser's *A Secret Life,* on the CIA's Polish asset Colonel Ryszard Kuklinski, is another.[9]

Some researchers have taken unconventional but still productive paths to a deeper insight on the evolution of the American intelligence system. David M. Barrett, for instance, mined congressional records, many of them in the papers of former members of Congress tucked away in local college libraries or historical societies (and holding a surprising amount of records that would be classified if residing in agency or departmental files).[10] American intelligence can also be studied through its relations with foreign intelligence services, as Jay Jakub and Richard J. Aldrich have demonstrated.[11]

News reports that are contemporaneous with the activity under scrutiny can be useful, when read with care. They are fragmentary and often wrong, but they have a certain vitality and immediacy, and they not infrequently touch on ground truth (sometimes better than reporters know). Hints of many intelligence operations show up in the newspapers during or shortly after they take place. A famous

example is the Chicago *Daily Tribune*'s story on June 7, 1942, which could have told anyone with a clue about intelligence that the Americans had broken Japanese naval codes in time to assist the U.S. Navy's defense of Midway Island three days earlier.[12] Parts of the *Tribune* article were shockingly accurate, but happily Tokyo either missed or ignored it. Indeed, the trouble for any outside observer is that of determining which of the myriad press reports accurately reflect real activities. This can be all but impossible to do, even for friendly intelligence officers reading in the papers about contemporary operations to which security compartmentation gives them no formal access.

Journalists who cover intelligence matters sometimes write histories of recent events—with mixed results. These tend to rely on anonymous sources whose motivations are left unexamined, to lack fastidious chronologies, and to seek to influence live policy debates. Not infrequently, moreover, they touch briefly on important issues or events but have little conception of their true significance. Thus these "instant histories" usually do not hold up well over the decades, and after a time they come to be viewed by scholars as being worth little more than extended newspaper articles.

Memoirs of intelligence professionals, and of decision makers who relied on them, are often useful, especially if the researcher remembers that no memoirist loses an argument in his or her own memorandum-for-the-record. There are very few "inside" memoirs, produced by a serving officer and written as part of the officer's official duties. Occasionally, a senior official will be given limited access to the files some years after retirement, and the manuscript written by the official will be sanitized to remove any classified information before it is published. More typical is the memoir produced with no access at all. A handful of memoirs are themselves small-scale intelligence operations—witness Kim Philby's *My Silent War*, published in 1968 while Philby was a pet of the KGB in Moscow.[13] His subtle mockery of CIA counterintelligence chief James Angleton—to name but one example—must be viewed according to how it may have served the KGB's interests to embarrass a pillar of its main enemy's defenses.

Oral histories should be heard in a similar light. There are a surprising number of former intelligence officers at large who can be (but usually have not been) interviewed. Indeed, at the time of this writing, there are a few hundred intelligence veterans of World War II still alive, a handful of them still working with U.S. intelligence organizations sixty years removed from the end of the war. This continuity (sometimes) allows researchers to have their drafts commented on by participants in the historical events, or at least by people who knew "how it felt" to do intelligence work in 1944, or 1964, or 1984. Oral history, however, falls in the same historiographical genre as the memoir literature and has to be judged by basically the same rules (indeed, when the subject of an oral history has died, the transcript of his or her interview is for all intents and purposes an informal memoir). The advantages and pitfalls of oral history are well known, however, and need not be reviewed here at greater length.

CONCLUSION

The last three decades have seen rapid progress in the methods of historical inquiry in intelligence in the United States. During this time the U.S. government has declassified millions of pages related to intelligence, a collectivity that is surely greater than that which any other nation has released on this subject. The two trends are related. Declassification has allowed historical scholarship of intelligence to make real strides, and scholarship has sometimes assisted declassification. The net result is that a large portion of the available "case studies" examined by scholars searching for the basic patterns of intelligence work tend to be American ones.

This is mostly a good thing, but it has its risks. Any researcher works with what he or she has, and thus the available sources will largely determine the research methods that can be employed. A great deal of reliable knowledge is being produced on U.S. intelligence for all phases of its existence—but the picture that has emerged is by no means a complete or balanced one. The material that has been declassified shows the controversies, not the daily grind, and thus it is a little skewed toward the extraordinary, just as reading only the morning newspaper could convince one that human life is an unending round of political controversies, violent crimes, movie openings, stock trades, and sporting events. Thus it also is with intelligence studies in the United States.

The results produced by the scholars working with these sources might well be expected to be quite insightful and detailed about particular incidents but not necessarily as learned about the whole sweep of American intelligence. It should not surprise us that a set of documents weighted toward "human intelligence" activities (as opposed to say, imagery intelligence), to analytical (vice operational) matters, and to happenings in Washington (as opposed to events in the field) gives rise to research that also concentrates on such matters. Academic and private scholars tend to focus on scandals, human intelligence (both espionage and covert action), and analytical debates. Their colleagues in the employ of the intelligence agencies not infrequently follow the example of their academic mentors and friends. The fact that the official researchers are employed by single agencies further weakens the incentive to do multiagency research, or to attempt to judge how well their agency and others worked together in advancing the national interest. There are fewer scholarly writings, with a less finely developed methodology, on the functioning of U.S. intelligence as a whole.

Such a judgment is not meant as a criticism of anyone engaged in the hard work of understanding U.S. intelligence history. What has happened is not the fault of outside scholars; it is the predictable corollary of official secrecy. Saying that, moreover, is not a condemnation of official secrecy, which is and must remain a reality. It is more an appeal to think beyond the sources, and the secrecy, and learn how to hunt for the proverbial car keys even in places where the

streetlight does not shine. What these methods amount to is a constant need to search for the impact that intelligence made on events. The researcher, both inside and outside the organization, must constantly ask what it was that an intelligence agency actually accomplished with the mission, resources, and authorities allotted to it. How well did it serve decision makers in their deliberations and the conduct of their offices? These are tricky questions to answer even with full access. Determining how well an agency worked with what was given to it is the intelligence scholars' contribution to achieving the ultimate goal of all intelligence scholarship: learning how intelligence made a difference.

NOTES

1. Kermit Roosevelt, ed., *War Report of the OSS*, two volumes (New York: Walker, 1976).; Arthur B. Darling, *The Central Intelligence Agency: An Instrument of Government, to 1950* (University Park: Pennsylvania State University Press, 1990); Laurance F. Safford, "A Brief History of Communications Intelligence in the United States," National Security Agency, 1952, available at http://www.fas.org/irp/nsa/safford.pdf.

2. Katherine A. S. Sibley, *Red Spies in America: Stolen Secrets and the Dawn of the Cold War* (Lawrence: University Press of Kansas, 2004).

3. See Kristian C. Gustafson, "CIA Machinations in Chile in 1970," *Studies in Intelligence* 47 (2003).

4. See Gerald Haines's addendum on this plot in Nicholas Cullather, *Secret History: The CIA's Classified Account of Its Operations in Guatemala, 1952–1954* (Palo Alto: Stanford University Press, 1999).

5. "My purpose is not to relate at length every motion, but only such as were conspicuous for excellence or notorious for infamy. This I regard as history's highest function, to let no worthy action be uncommemorated, and to hold out the reprobation of posterity as a terror to evil words and deeds." Tacitus, *Annals*, III:65.

6. This Church Committee volume was drafted by Anne Karalekas and later republished in a volume edited by William M. Leary, *The Central Intelligence Agency: History and Documents* (Tuscaloosa: University of Alabama Press, 1984).

7. *New York Times*, editors, *The Pentagon Papers as Published by the New York Times* (New York: Quadrangle, 1971); "The CIA Report the President Doesn't Want You to Read," *Village Voice*, supplement, 11 and 23 February 1976.

8. Peter Grose, *Operation Rollback: America's Secret War Behind the Iron Curtain* (New York: Houghton Mifflin, 2000); Kathryn S. Olmsted, *Red Spy Queen: A Biography of Elizabeth Bentley* (Chapel Hill: University of North Carolina Press, 2002).

9. Evan Thomas, *The Very Best Men: Four Who Dared—The Early Years of the CIA* (New York: Simon & Schuster, 1995); Benjamin Weiser, *A Secret Life: The Polish Officer, His Covert Mission, and the Price He Paid to Save His Country* (New York: Public Affairs, 2004).

10. David M. Barrett, *The CIA and Congress: The Untold Story from Truman to Kennedy* (Lawrence: University Press of Kansas, 2005).

11. Jay Jakub, *Spies and Sabotuers: Anglo-American Collaboration and Rivalry in Human Intelligence Collection and Special Operations* (New York: St. Martin's, 1999);

Richard J. Aldrich, *The Hidden Hand: Britain, America and Cold War Secret Intelligence* (London: John Murray, 2001).

12. Gordon W. Prange (with Donald M. Goldstein and Katherine V. Dillon), *Miracle at Midway* (New York: McGraw-Hill, 1982), p. 367. Subsequent legal and Congressional probes that summer exposed the fact of a breakthrough in reading Japanese codes.

13. Kim Philby, *My Silent War* (New York: Grove, 1968).

7

THE CHALLENGES OF INTELLIGENCE ANALYSIS

JOHN HOLLISTER HEDLEY

ANALYSIS FITS INTO THE NATIONAL INTELLIGENCE PICTURE as the finished portrait of an intelligence subject—perhaps a snapshot of a fast-breaking development, perhaps a product of collaborative, in-depth research. Reporting an event is one thing; answering the question "what does this mean?" is analysis. Analysis goes beyond what happened—as best we can discover what happened—to assess what to make of it. Analysts do both when they write: They report and they assess. What they write constitutes the intelligence product, or "finished intelligence." This product may take the form of a quick-reaction commentary, an assessment of an event's likely implications in the near term, or a study of long-term trends and their potential consequences. In every such instance, intelligence analysts every day are striving to make sense out of often ambiguous, inconsistent, incomplete, and sometimes contradictory data. And they do so not in a seminar but in the fast-breaking world of foreign and defense policy.

Richard Helms, whose long career in intelligence operations culminated in seven years as the Director of Central Intelligence, put it this way: "It is a long span from secret reports and photos to the conclusions reached by Washington intelligence analysts, men and women sitting at desks sorting, sifting, and patterning secret evidence into a matrix that carries conviction. This work—analysis—is the bottom line of intelligence work. This is where all the arcane techniques of intelligence come together. This is the unknown, the neglected side of the profession that has been caricatured into absurdity by writers of spy thrillers."[1] Helms, no writer of spy thrillers but himself a spy of the first order, knew that timely, objective analysis is the end result of all the activities that go into the acquisition of intelligence information.

Helms's observation, made decades ago in the midst of the Cold War, is equally true in the 21st century. The attacks of September 11, 2001, on the World

Trade Center in New York and the Pentagon in Washington underscored the growing challenges to intelligence in an era of international terrorism in which small groups of individuals can inflict destruction once wielded only by nation-states. Indeed, this look at the nature and challenges of intelligence analysis comes as the bureaucratic dust still is settling following the hasty, election-year enactment of the Intelligence Reform and Terrorism Prevention Act of 2004, which was an outgrowth of those attacks. That legislation created the position of Director of National Intelligence as an institutional corrective for the failure of the vast U.S. national intelligence apparatus to somehow prevent the terrible events of 9/11. The reorganization followed the completion of various inquiries and studies into what went wrong.[2] The general, overriding conclusion of these inquiries with respect to intelligence analysis was that there had been a failure of imagination—that analysis tended to be risk-averse and more concerned with avoiding mistakes than with imagining surprises—and that there was insufficient integration of analytic efforts across the now sixteen-member U.S. intelligence community. The Office of the National Director of Intelligence now is at pains to emphasize consultation and collaboration in intelligence analysis. The office is providing central direction aimed at rising above the bureaucratic fiefdoms that for years formed barriers to the sharing of sources and analytic perspectives. Mental roadblocks to more imaginative analysis, however, are persistent challenges discussed below.

The essence of analysis is information plus insight, derived from subject-matter knowledge. It should be clear from the outset that there is nothing nefarious about trying to know and understand as much as possible about what is going on in the world. And this is the purpose of analysis: to discern pertinent facts from a flood of information and apply judgments and insights that can inform those who must make decisions and direct actions to address developments on a global scale. Intelligence analysis informs decisions and actions in ways that can make a positive difference. Timely intelligence warns of looming crises, identifies threats, monitors fast-breaking situations, illuminates issues, and detects trends. Intelligence helps U.S. policy makers consider alternative options and outcomes.

TYPES OF INTELLIGENCE

The grist for the analyst's mill is a mix of all the kinds of information the U.S. government is able to acquire. Much of the information is openly available in print or electronic form, including the Internet, newspapers, television, radio, journals, commercial databases, videos, graphics, maps, and drawings. A critical amount of intelligence information, however, is obtained from highly sensitive sources. These include:

Human-source intelligence, acquired openly by civilian and military personnel assigned to U.S. diplomatic posts, through official liaison contacts with other intelligence services, by debriefing foreign nationals and U.S.

citizens who travel abroad and have access to information of intelligence value; it is acquired clandestinely by recruiting foreign agents with unique access to the hardest targets of all: not just documents but the people who make policies and operational plans—and if possible, recruiting those people to be agents themselves.

Signals intelligence, derived from intercepted communications, radar and telemetry.

Imagery intelligence, whether obtained overhead from satellites or aircraft or from the ground.

Measurement and signature intelligence, involving a range of disciplines including nuclear, optical, radio frequency, acoustic, seismic, and materials sciences that can locate, identify, or describe distinctive characteristics of intelligence targets.

Complicating the mix of these secret sources of intelligence reporting is its sheer volume, its rapid-fire receipt, the ever-present "noise" of contradictory and inaccurate information, and deliberate deception designed to mislead.

The fact that analysts do "all-source analysis" reflects the reality that rarely is one source from a single one of these collection categories sufficient. Sources need to be supplemented and complemented to be as complete as possible and to be verified to the greatest extent possible. Research and analysis in open sources may turn up information, for example, on the strategic perspective of *jihadist* movements. But because these groups attach highest priority to the security of their communications and operations, it is difficult to identify leaders and uncover decision making and attack planning. It is likely to require the full range of intelligence collection capabilities to penetrate operations by cells of a few isolated individuals whose fluid movements are "beneath the radar." In making analytic judgments, the analyst facing a deadline yearns for additional sourcing. But actually having multiple sources to corroborate each other is the ideal. It is by no means the rule, and multiple sources can in some instances still lead you astray. Indeed, one of the differences between intelligence writing and academic writing is having to write before you feel ready to do so, before you have marshaled the supporting evidence you want to have in order to craft your position. In this sense, writing current intelligence is very much like being a newspaper reporter or columnist: When it's time to go to press, you have to have your material ready to go.

READYING "FINISHED" INTELLIGENCE

Intelligence analysis is the culmination of the intelligence process, although the process actually is a never-ending cycle. Analysis drives collection by identifying information needs and gaps, which in turn call for more collection, which requires further analysis. What the key recipients of intelligence analysis—the

president, the National Security Council, and senior officials in major departments and agencies—must be aware of, grapple with, or defend against in the world around us dictates collection requirements. They reflect the core concerns of national security policy makers and military commanders who need timely, reliable, and accurate foreign intelligence information—especially the kinds of information that are not readily available. As analysts address those needs from day to day, they identify and prompt the collection mission again and again.

Before the raw data that human or technical collectors acquire can be analyzed, however, some interim processing and exploitation may be required to convert "raw" data into a usable form for analysis. It may be necessary, for example, to decrypt or translate intercepts, or to interpret images through highly refined photographic and electronic processes. Although personnel involved in this processing sometimes are referred to within their organizations as analysts, their specialized work—involving judgments about relevance and priority within a single collection category—is not the production of "finished" intelligence.

Although producing intelligence is a dynamic, never-ending process, the term *finished intelligence* refers to any intelligence product—whether a one-paragraph bulletin or a lengthy study—that has completed the rigorous, all-source correlation, integration, evaluation, and assessment that enables it be disseminated. As we have noted, the intelligence analyst who is the author of such a product is expected to have checked it against intelligence information from all sources pertinent to his or her area of responsibility. The analyst will have assessed its validity and determined—with the substantive and editorial help of experienced managers and colleagues—that it can usefully advance its recipient's knowledge and understanding of a pertinent security policy issue.

Finished intelligence is made available in several forms, and analysts can expect to be called upon to produce in any or all of them:

> *Current intelligence* addresses day-to-day events—new developments and possible indicators of developments to come. Current intelligence not only reports intelligence information but assesses its significance, alerts readers to near-term consequences, and signals potentially dangerous situations. Current intelligence is disseminated daily. Sometimes it appears even more frequently, in the form of situation reports from a task force formed to deal with a crisis. Often it takes the form of ad hoc written memoranda and oral briefings. The *President's Daily Brief* is the most elite example of current intelligence, but other highly sensitive publications for the most senior levels of government and the military appear daily, weekly, or on request.
>
> *Estimative intelligence* takes stock of what is known and then delves into the unknown, even the unknowable. International issues rarely are conclusive, yet policy makers must address them with plans and decisions. Estimative intelligence provides strategic guidance for developing policies, usually looking three to five years ahead. It suggests alternative patterns that

available facts might fit and provides informed assessments of the range and likelihood of possible outcomes. The most formal and authoritative form of estimative intelligence is a national intelligence estimate, which the pertinent organizations of the intelligence community prepare collaboratively and issue collectively.

Basic intelligence compiles reference data—biographic, geographic, military, economic, demographic, social, and political—presented in the form of monographs, in-depth studies, atlases, maps, order-of-battle summaries, and publications such as *Chiefs of State and Cabinet Members of Foreign Governments* and an annual *World Factbook* that is a comprehensive compilation of political, economic, and demographic data.[3]

Other types of finished intelligence include *warning intelligence* (which necessarily should be timely), designed to highlight threatening events that would require a potential policy response and that could cause the engagement of U.S. military forces, and *intelligence for operational support,* which, as the name indicates, is focused and tailored for the planning and conducting of a specific operation. *Scientific and technical intelligence* assesses technical developments and characteristics, and the capabilities and performance of foreign technologies including weapon systems. Technical analysis usually relates to defense planning, military operations, or arms-control negotiations.

None of these types of finished intelligence, however, brings the process to a conclusion. Whether a daily item or a national estimate, their production is part of a continuum that involves dissemination, feedback, and more questions that fuel a truly dynamic effort.

What's more, whether current or longer term, the analytic interpretation of intelligence reporting requires making judgments that go beyond the available information. Such a leap, from the information at hand into a meaningful analytic product, inevitably involves venturing from the known into the uncertain. Almost by definition, intelligence analysis involves confronting uncertainty. The analyst is commonly working with incomplete, ambiguous, and often contradictory data and must use his or her judgment—and subject-matter expertise—to transcend its limits.

THE WORK ENVIRONMENT

The climate in which analysts work has changed dramatically from the early decades of the U.S. intelligence community's existence. During the Cold War that dominated the second half of the 20th century, the analytic challenge was often one of having too little data. The Soviet Union and its allies were closed societies going to great lengths to deny information. They denied travel, controlled the press, and jammed radio broadcasts. E-mail and cell phones did not exist. U.S. intelligence agencies had a virtual monopoly on the information that

was collected, essentially secret information obtained by agents, communication intercepts, or overhead photography, and there never seemed to be enough. In the 21st century, a principal analytic challenge lies in the sheer volume of information available. Although especially hard targets such as terrorist cells are no less difficult to penetrate, the explosion of open-source information from news services and the World Wide Web makes the speed and volume of reporting more difficult to sift through. Advances in information technology both help and hinder, as analysts strive to cope with the "noise," the chaff they must winnow through. Data multiplies with dizzying speed. Whereas collecting solid intelligence information was the overriding problem of the past, selecting and validating it loom ever larger as problems for analysts today.

To a degree perhaps surprising to someone new to the inner sanctum of a Washington intelligence organization, the working climate that does not change is that which walls off the workplace from the bluster of partisan politics. Analysts must check their personal political views at the door. Objectivity is the analyst's by-word, intellectual honesty the core value. The policy-making customers that analysts seek to inform—all the way to intelligence customer number one—need to get the straight scoop, unvarnished and politically neutral.

The author has been directly involved in producing intelligence for eight presidents—five Republicans and three Democrats. Whatever the partisan rhetoric or the legislative agenda, without exception they all have been serious and conscientious about their role in foreign policy and as commander in chief, and they take seriously the intelligence that can inform their efforts. They have the best of intentions, and although they obviously differ in style, approach, and effectiveness, they want and need the best intelligence they can get. (So, for that matter, does the Congress. And the congressional oversight committees—the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence—by and large score well on bipartisanship, especially behind closed doors and apart from public rhetoric.)

Accordingly, an analyst is much the wiser and more effective by not taking sides on the job. No matter how much one might personally wish to see expanded healthcare on the one hand or tax cuts on the other, when it comes to helping the government better understand what is going on in the world, the only rule to follow is to be scrupulously objective. As the umpire advised, "call 'em as you see 'em." There is no room in intelligence analysis for partisan advocacy or opposition when providing actionable intelligence and identifying options. In short, you don't bend things to fit the way you'd like things to be. This will always catch up with you, and your credibility is what will suffer.

IT'S ABOUT WRITING

What the analyst needs to bring to the job is an open mind and an ability to think and write clearly. Oral briefings are valued and often called for. But

ultimately, writing is what the analyst's work is about—writing based on organizing material, conceptualizing, and thinking critically about it. Writing is always done with the audience—the reader—in mind. And the writing analysts do is different from that learned and practiced in the professorial ranks of graduate school, even though there are many similarities between the intelligence field and academia.

Like academicians, intelligence analysts attach the highest importance to knowledge and understanding, to objectivity in the search for truth, and to accuracy in the sources they use. Academics and analysts are interested in clear descriptions and explanations, though academics usually are describing past events and making sense of what happened, while analysts are addressing what an event means and projecting what might happen next. They tend to differ when it comes to the material they work with, and their likely audience. Academic authors organize their data, make it as comprehensive as possible, reflect on it, develop a theoretical construct, and perhaps formulate methodologies. For the analyst—especially one writing current intelligence—this approach is likely to be an impossible luxury. As Douglas MacEachin, former Deputy Director for Intelligence—the head of analysis—at the Central Intelligence Agency (CIA) has put it, "one group gets to promote its reputations in journals, while the other works in a closed environment in which the main readers are members of the world's most challenging audience—the policymaking community."[4] The analyst may need to write for the next morning's publication, or contribute to this afternoon's situation report, on a development for which data is sorely lacking. There is not enough data to work into a meaningful methodology, and there is no waiting for more data: The deadline must be met with whatever can be said.

Whereas academics usually write—particularly in the case of journal articles—for other scholars with a shared expertise, analysts usually write for nonexperts who do not share their expertise and who do not have time for in-depth study or to follow an issue day in and day out to the degree the analyst does. Analysts therefore are called upon to bridge the gap between the specialist and the generalist. Getting the attention of senior officials—from the president to an under secretary—who, by the breadth of their responsibility, are forced to be generalists, may mean the analyst has one page, or two or three minutes, in which to make sense of a development. No matter that, ideally, putting this development into historical perspective and into its international context should require considerable background reading and careful study and reflection. There is no such option. However much the generalist reader might benefit from a scholarly tutorial, he or she simply will not sit still for one. Even if you write the kind of paper you would like the policy maker to have in order to get a more comprehensive exposition of what is at issue, it probably will not be read at the highest level. So to reach the reader at that level, the analyst must take the opportunity that is available: one page or nothing, three minutes or none.

Different audiences dictate a different style. And the first rule of persuasive writing is to know your audience. For busy readers, shorter is usually better. The analyst's policy-maker audience is unbelievably pressed for time, which may or

may not be the case for the scholar reading the academic's work. The analyst's audience determines the writing style, and the one that is most effective for the generalist reader—whether the president, chairman of the joint chiefs, or a cabinet officer—is simple, crisp, readable prose. Good journalistic writing is a good example. (Read Tom Friedman columns in the op-ed section of the *New York Times*, and "What's News" on the front page of the *Wall Street Journal*.) What is written must be easy to grasp in a quick reading. Editors, as a surrogate first reader, can provide indispensable help. But sometimes, finished intelligence must be done on the run and off the cuff. A friend who was an analyst in the State Department's Bureau of Intelligence and Research remarked that the bureau's most effective analytic "product" often was a one- or two-sentence comment on a report in the secretary of state's morning briefing, perhaps followed by one or two short paragraphs the next day. The *President's Daily Brief* keeps items to a single page, sometimes less, with a lot of white space. Always, intelligence writing puts a premium on being able to state key points quickly, succinctly, and with clarity. Restrictions on time and space require an economy of words.

NEW DEMANDS

Demands on the intelligence analyst—and the expectations—are increasing. Everyone is overwhelmed by information. Policy makers are looking to intelligence to help them know what they should be worrying about, what they should be addressing, and what their options and their likely consequences are. They have insufficient time to read or to contemplate, so helping them cope with the flood of information has become a major service analysts provide. Policy makers value the ability of the intelligence analyst to integrate data with no axe to grind.

All the while, the analyst's customers grow ever more numerous and more sophisticated. Recipients of intelligence analysis who have newspapers and press summaries on their desk and CNN on the air wherever they go have a high level of awareness. And no one ever wants less intelligence, in terms of products, briefings, or coverage—only more and better. Congress has an insatiable appetite for intelligence, as do the military services. Executive branch customers abound in the Departments of the Treasury, Energy, Justice, Homeland Security, Commerce, and Agriculture.

What the analyst writes must compete for attention with multiple sources of information and other intelligence producers. The trick is not to cheapen the currency by inundating the reader but to be timely, relevant, and to provide value added—even when addressing a much-reported issue of the day. Intelligence analysis needs to contribute uniquely, going beyond what's in the news media. And of course it is worthless if it doesn't arrive when it can be used.

Although policy makers—especially when a new administration takes office—insist that they want long-term projections that will help them plan wise policies, their attention invariably becomes riveted on the here and now. The fact

that developments worldwide are reported in real time contributes to an atmosphere of perpetual crisis, of needing to respond instantly to anything and everything—an atmosphere in which current intelligence carries the day.

The fact is, decision makers want and need both strategic and current analysis. Critics and commissions of inquiry post-9/11 comprise a veritable chorus of conventional wisdom decrying an overemphasis on current intelligence working to the detriment of in-depth analysis. The appeal is being heard and acted upon. The National Intelligence Council, for example, already a center of strategic analysis that leads intelligence community projects and works with outside experts, has added a unit to lead interagency analysis on long-term and underexamined strategic issues that would be walled off from current demands.

Whether current or longer term, the desire on the part of the users of intelligence is for analysis that is opportunity-oriented, or actionable—in other words, intelligence they can apply and actually use. Analysis has become an integral part of planning and implementing policy, and of intelligence operations. This is a far cry from what might be termed the traditional, or "old school," conception of analysis, which held that, to be policy neutral, analysts literally had to keep their distance from those who were making the policy decisions. Traditional thinking also held that analysis, to be scrupulously objective, should be done independently of those who collect it.

COLLABORATING BUT NOT POLITICIZING

For a number of years, the trend has led away from this traditional view for a variety of practical reasons. Working in isolation only increased the guesswork involved in discerning what policy makers needed to know and thus what collectors needed to collect. In contrast, working collaboratively enables analysts to get an invaluable "feel" for what information the policy maker is missing. Learning first-hand the information needs and priorities of the day helps analysts guide what the collectors must target. Collectors can have a real-time sense of what to collect and analysts can have a sharper awareness of what they have to work with and of the illumination and insights they must try to provide.

Today, analysts and policy makers meet together regularly and frequently from the highest levels—the deputies committee and principals committee meetings that prepare for national security council meetings with the president—to various gatherings at the working level. At the CIA, analysts sit side by side with HUMINT collectors in the operations directorate now known as the National Clandestine Service. They do so as well at the various centers where analysts and collectors can better focus and share their combined efforts—such as the National Counterterrorism Center, the National Counterproliferation Center, and the International Crime and Narcotics Center.

How analysis informs policy might be answered with "very carefully." Analysts must walk a fine line not to be prescriptive. They must illuminate

alternatives but not suggest which one to take. Their collaboration with policy makers and collectors increases the risk of politicizing intelligence and, accordingly, raises the pressure on analysts to resist it. Tailoring intelligence by no means involves slanting its content to curry favor with its recipient; it means making it as relevant as possible by addressing as precisely as possible the policy maker's particular information needs. The analysts' highest calling is to speak truth to power. They must convey assessments that the policy makers surely will not want to hear.

In the process, analysts must resist the temptation to "cherry pick" intelligence items to provide, even though no one should be surprised that policy makers, for their part, "cherry pick" from the intelligence they receive. Policy makers may point publicly to that which seems to support their policy and disregard that which does not. But woe unto the analyst who would cherry pick intelligence likely to please the policy recipient and suppress that which would not. Such a practice would quickly come to light and would cost the analyst's credibility, which is the indispensable currency of the analyst's realm.

Bias may happen, but nobody instructs you to change your interpretation. This author can honestly say that, as a line analyst at CIA, as a manager of analysts, as managing editor of the *National Intelligence Daily,* and in editing the *President's Daily Brief*, he personally never experienced pressure from any superior officer to alter any analytic judgment to suit a policy line. He has, however, seen a very few instances in which analysts, convinced that their viewpoint was the embodiment of truth, became knee-jerk apologists or advocates for a position or outlook—to an extent that they were no longer seen as objective and open-minded, and whose analytic careers effectively ended as a result.

Today, analysts have to be ever mindful that they must somehow maintain an invisible firewall separating the informing of policy from prescribing policy, even as they work hand in glove with both policy makers and collectors in order to more effectively identify knowledge gaps and strive to fill them. The idea is to support the process of making policy by identifying options that help serve all players and leave to the policy makers the responsibility for charting the course.

PITFALLS

The post-9/11 studies also emphasized anew what analysts have grappled with for years: the fact that, as human beings, we all have cognitive bias or preconceived notions that we must acknowledge and be wary of lest they color our perceptions and our judgment. We all are culture-bound in our outlook and must consciously strive to recognize this fact and rise above it.

Some of the particular pitfalls the analyst must constantly strive to avoid include:

"Clientitis," or the tendency to fall in love with your "client," the country you may be assigned to cover, is a sophomoric sin but one that is not

unknown. Developing expertise obviously means knowing a great deal about a country, usually involving extensive travel and often some time in residence. Analysis involves discerning and explaining the motives and point of view of its leaders. But admiration for its language, customs, and culture must not lead the analyst to become the advocate and defender of its leaders and their policies. Objectivity must reign supreme.

Mirror-imaging is the assumption that others would think just the way you do—that, being confronted with the facts of a certain situation, they would calculate the pros and cons and decide their course of action with the same reasoning, and thus reach the same conclusion. (Anthropologist Rob Johnston points out that this term actually is a misnomer, inasmuch as a mirror image is a reverse image. He uses *ethnocentrism* to describe the concept that we tend to perceive foreigners—friends or adversaries alike—as thinking the same way as Americans. He also notes that "trying to think like them" often results in applying the logic of one's own culture and experience to try to understand the actions of others, without knowing that one is using the logic of one's own culture.[5])

Mindset is the tendency to evaluate newly acquired information through an existing hypothesis, rather than using new information to reassess the premises of the hypothesis itself. Douglas MacEachin, former head of CIA's analysis directorate, explains how this happened to analysts trying to determine if or when the Soviet Union would invade Afghanistan in early 1979. Once having judged what the Soviets would require for an invasion force and thus what military indicators would presage an invasion, analysts disregarded indicators that did not fit that judgment.[6]

Groupthink is the inclination to have one's interpretation reinforced by others coming to the same conclusion. As other analysts arrive independently at the same hypothesis, or simply accept and thereby endorse yours, the analyst is tempted to consider the assessment confirmed. Groupthink thus helps form or reinforce mindset.

Linear analysis presumes a straight-line, sequential projection in which one development appears to flow logically from that which preceded it. An oversimplified illustration is that if we know, for example, that Saddam Hussein had weapons of mass destruction, we know that he tried in several ways to obtain more of them, and that he is successfully concealing what he has done subsequently, linear analysis would lead one to conclude that what he has done subsequently is acquire more weapons of mass destruction. Linear analysis does not allow for the unexpected outcome. As Princeton professor Robert L. Hutchings—former chairman of the National Intelligence Council—put it, "Linear analysis will get you a much-changed caterpillar, but it won't get you a butterfly. For that you need a leap of imagination."[7]

An old example is still one of the best examples of mirror-imaging. The most dangerous superpower confrontation of the Cold War posed the analytic question of whether or not the Soviet Union would send offensive missiles to Cuba. The judgment of analysts across the U.S. intelligence community was that a rational actor would not do this, that Soviet leader Nikita Khrushchev would know better than to run such a risk. Yet he sent the missiles on their way. Ironically, the U.S. analysts ultimately were right and Khrushchev was wrong. Sending the missiles was a major error. His humiliating withdrawal of them contributed to his ouster. But the analysts' misjudgment points up the need to be skeptical of a "rational actor" model. The Soviet leader did not see the risk equation in the same way. In the end, it was our insufficient understanding of his psychology and world view that led us to believe the act of sending the missiles would be an irrational option.

Analysts have on a number of occasions been surprised by what seemed from the U.S. perspective to be irrational decisions by foreign leaders. Soviet tanks crushed the reformist government in Czechoslovakia in 1968 when it did not seem in Moscow's interest to do so. In 1973, U.S. (and Israeli) intelligence analysts concluded that it made little sense for Egypt and Syria to attack Israel, given the military inferiority of the Arab side as demonstrated in the 1967 war. It seemed irrational for Saddam Hussein to invade Kuwait in 1990, and for India to explode a nuclear bomb in 1998. But the decision maker who counted did not see these actions as irrational. (Who knows if Saddam's analysts concluded in 2003 that the United States was only bluffing and would not actually invade Iraq!) Getting out of one's Western mindset is always difficult, but it is critical if we are to assess correctly the motives and policies of foreign leaders.

The controversial analytic estimate in September 2002 concerning Saddam Hussein's weapons of mass destruction contained a "perfect storm" of analytic pitfalls. Virtually all of them—mindset, groupthink, and linear analysis—were in evidence to some degree, resulting in a warning for the ages to be wary and to question the conventional wisdom. As a British scholar describes it, the groupthink consensus that Saddam was stockpiling weapons of mass destruction was formed

> despite the intelligence community's own agreed assessments that the evidence didn't indicate that he was, or, for that matter, that he wasn't, since the information was too fragmentary to know with certainty and Saddam too mercurial to predict with confidence. The consensus at work had its roots not in raw intelligence or other substantive evidence but in unanswered questions and political assumptions.[8]

It is easy, of course, to cite instances in which U.S. intelligence assessments missed the mark. The news media do so rather gleefully. It is the nature of their business, just as missing the mark is in the nature of the intelligence business. More than twenty-five years ago, Columbia University scholar Richard Betts asserted that intelligence failures are not only inevitable, they are natural.[9] They still are, and will continue to be, because to do their job well, intelligence analysts

must be willing to take risks. No matter how incomplete, inadequate, uncertain, or contradictory the information on which a judgment must be made, the judgment is nevertheless expected and must be made. And making it necessarily entails a recognition of the risk that the judgment can miss the mark.[10]

Sherman Kent, a former professor of European history who in a thirty-year career in intelligence earned a reputation as perhaps America's foremost practitioner of the analytic craft, was directly involved in the classic misjudgment at the outset of the Cuban missile crisis. Reflecting on it later, Kent asked rhetorically how it could have happened. "The short answer," he wrote, "is that, lacking direct evidence, we went to the next best thing, namely information which might indicate the true course of developments."[11] The reader should mentally underline "might." As Kent put it, if a national intelligence estimate "could be confined to statements of indisputable fact, the task would be safe and easy. Of course the result could not then be called an estimate."[12]

There is no bureaucratic reorganization that can solve once and for all the problem of preventing intelligence misjudgments, because uncertainty itself is the problem. The inevitability of intelligence failures—if this means not predicting exactly when and how something might catch the United States by surprise—virtually has the certainty of a law of physics. No one can predict the future, and no one person or organization can be right on all subjects at all times. Allegations of intelligence failure therefore are inevitable, in large part because, in intelligence, failures are inevitable. And failures are trumpeted whereas successes often are publicly unknown. Analysts have to accept this as the cost of doing business. But rest assured that intelligence often is on target. Presidents would not insist upon it as a daily diet and Congress would not demand and fund it if it were not of value. Much of the value is incremental and does not come in dramatic, bolt-from-the-blue revelations, but the value is there. And it is a safe bet that it is best produced by analysts who park their preconceptions at the door, constantly review indicators from all sources, question conventional wisdom and their own assumptions (especially if analytical consensus emerges quickly), and weigh alternative explanations.

Human nature being what it is, the various pitfalls discussed above will surely continue to challenge an objective perception and explanation of events. But there is help, both in preparing for the challenge and in meeting it on the job. It is unlikely that anyone will walk into an organization in the U.S. intelligence community without having to learn and practice the tradecraft. At CIA, home of the intelligence community's largest analytic component, the creation by the year 2000 of the Sherman Kent School of Intelligence Analysis testified to an intensive effort to teach the tradecraft of intelligence analysis. Experienced intelligence officers with extensive analytic experience run a Career Analyst Program for new analysts, who now spend their first five months with the Agency developing the specialized thinking, writing, and briefing skills of intelligence analysis. Interim assignments enable them to apply themselves in various jobs throughout the Agency and elsewhere in the intelligence community.[13] On-the-job training

continues throughout an analyst's career. Supervisors provide mentoring. Peer review helps shape their research effort and critique their preliminary findings. The professionalizing of today's analysts emphasizes the use of multiple hypotheses and various alternative interpretations of trends and indications. The Office of the Director of National Intelligence promotes critical discussion among analysts throughout the intelligence community in addressing analytical challenges. Editorial reviews help ensure that analysts communicate their message clearly.

Personality and temperament also factor into what makes an effective analyst. Those who would work in current intelligence assignments, especially, must be able to work with short deadlines. Structure and predictability may be in short supply. What is guaranteed is a diet of long hours under pressure, and a need to be responsive and flexible. In-depth research requires sifting through mounds of data, and conceptualizing from that data calls for hard study, developing and bringing to bear one's substantive knowledge, and doing deep thinking for long stretches. But what also is guaranteed is an unparalleled opportunity to know more about what is happening around the globe. Excitement may not be constant, but a flow of adrenalin and a sense of satisfaction characteristically accompany the work of intelligence analysis. It opens a unique window on world affairs. It offers the prospect that one person's contribution can make a difference in American foreign policy. Analysts who write an item that runs in the *President's Daily Brief* know that their judgment is appearing in the publication with the smallest and most influential subscription list in the world. Joining forces throughout the U.S. intelligence community, analysts illuminate complex issues, detect patterns, identify targets, and increase the U.S. government's understanding of far-flung developments. It is a high calling, a fascinating profession, and a pursuit that can contribute significantly to national security.

NOTES

1. Foreword to Russell Jack Smith, *The Unknown CIA* (Washington, DC: Pergamon-Brasseys, 1989), pp. ix, x.

2. See, for example, *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: Barnes and Noble, 2004), and *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Washington, DC: US Government Printing Office, 2005). Recommended as the best single assessment of the 9/11 Report and the consequent rapid congressional and White House response manifest in the Intelligence Reform Act is Richard Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11* (Lanham, MD: Bowman and Littlefield, 2005).

3. *Chiefs of State and Cabinet Members* and the *World Factbook* are published both in classified and unclassified versions, the latter for public use and available on CIA's website.

4. Foreword to Richards J. Heuer Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), p. xi.

5. Rob Johnston, *Analytic Culture in the U.S. Intelligence Community* (Washington, DC: Center for the Study of Intelligence, 2005), pp. 75–76.

6. Douglas J. MacEachin, *Predicting the Soviet Invasion of Afghanistan: The Intelligence Community's Record*, monograph published by the Center for the Study of Intelligence, 2002.

7. Robert F. Hutchings in the Preface to *Mapping the Global Future* (Washington, DC: National Intelligence Council, 2004), p. 1.

8. Philip H. J. Davies, "Intelligence Culture and Intelligence Failure in Britain and the United States," *Cambridge Review of International Affairs* 17 (October 2004), p. 517.

9. Richard K. Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics* XXXI (October 1978), reprinted with permission in *Studies in Intelligence* 23 (Fall 1979), p. 54.

10. John Hollister Hedley, "Learning From Intelligence Failures, *International Journal of Intelligence and Counterintelligence* 18 (Fall 2005), p. 437.

11. Sherman Kent, "A Crucial Estimate Relived," originally appearing in the classified Spring 1964 issue of CIA's internal journal, *Studies in Intelligence*, republished in *Studies in Intelligence* 35 (Winter 1991), p. 67.

12. Ibid., p. 65.

13. John Hollister Hedley, "The DI: A History of Service," in *Fifty Years of Informing Policy* (Washington, DC: Directorate of Intelligence, 2002), p. 17.

8

THE INTELLIGENCE-POLICY NEXUS

JAMES J. WIRTZ

INTRODUCTION

THE INTELLIGENCE-POLICY NEXUS IS A CRITICAL PART of modern government. Policy makers rely on intelligence professionals for data about broad international trends and their potential consequences, information about the intentions and capabilities of friends and foes alike, and specific warnings needed to avert disaster. Intelligence managers and analysts look to the policy establishment for their raison d'être. The intelligence community exists solely to provide policy makers with the information and analysis needed to formulate effective public policies. Few relationships in government are as symbiotic as the intelligence-policy nexus. One might thus expect that it would be relatively easy for intelligence professionals and policy makers to maintain smooth and productive working relations. Yet, few relationships are as challenging or produce as much controversy as the interaction between policy makers and intelligence professionals. The modus vivendi that governs their work is fragile, and disagreements that originate deep within the bureaucracy can easily find their way into tomorrow's headlines. The accusation that the Bush administration manipulated finished intelligence to support the decision to launch a preventive war against Iraq in 2003, for example, is the latest contentious issue in the history of the intelligence-policy nexus in the United States.

A variety of problems can emerge to bedevil relations between the intelligence and policy-making communities. The best-known pathology, politicization, occurs when policy makers place overt or subtle pressure on intelligence analysts and managers to produce intelligence estimates that support current political preferences or policies. Other issues, however, have received far less

attention in the literature on intelligence. For example, there is no consensus about what constitutes best practices when it comes to intelligence-policy interaction, which can lead to acrimony as intelligence managers attempt to institute reforms. The information revolution also is creating new points of friction as intelligence analysts and policy makers interact using informal channels of communication, creating new challenges for those charged with monitoring the contents of finished intelligence—formal written reports that reflect a deliberate judgment made by analysts.

This chapter explores the tensions and pressures that shape interaction between intelligence professionals and policy makers as they go about the business of informing, making, and executing foreign and defense policy. The first section describes the two normative theories that offer competing explanations of how relations between intelligence professionals and policy makers should be organized. It also explores the intelligence pathologies that can emerge if either of these theories is applied with too much stringency. The second section explores the origins and consequences of politicization. The third section examines how the information revolution is transforming the relationship between analysts and officials, producing benefits as well as unintended consequences. Although technology has always shaped the intelligence cycle—setting intelligence requirements, collecting data, analyzing information and producing finished intelligence, and communicating information to people who can put it to good use—the information revolution might actually be altering the intelligence-policy nexus, creating an entirely new dynamic in relations between the intelligence and policy-making communities.

A THEORY OF THE INTELLIGENCE-POLICY NEXUS?

Two normative theories animate the debate about best practices in the intelligence-policy nexus. One, most closely associated with the work of Sherman Kent, focuses on ensuring the independence of intelligence analysts when it comes to providing information to policy makers.[1] Kent's thinking, which shaped the formation and early evolution of the U.S. intelligence community, identifies the importance of political and policy detachment when it comes to producing relevant and effective finished intelligence. The other operational framework, most closely associated with the reforms instituted in the mid-1980s by then Director of Central Intelligence Robert M. Gates, focuses on providing "actionable" intelligence, information of immediate and direct use to policy makers.[2] To produce actionable intelligence, analysts have to maintain close working relationships with policy makers, literally looking into officials' inboxes to make sure finished intelligence addresses important policy issues of the day. These frameworks appeal to different groups within the government, produce specific benefits, and exhibit unique intelligence pathologies.

The Kent Approach

Sherman Kent's approach to the intelligence-policy nexus is based on the premise that effective intelligence is independent intelligence. Analysts must maintain their distance from current policy and policy makers to prevent their reports from being shaped by their customers' preferences. In Kent's view, intelligence managers and analysts should be free to set intelligence requirements and production plans for finished intelligence products, deciding which projects best support policy makers. This approach guards against politicization because it creates real procedural and even physical barriers that prevent policy makers from influencing the questions addressed and answers presented in finished intelligence. Analysts often champion this model of the intelligence-policy nexus because it provides them with the intellectual freedom to pursue their interests within the relatively broad guidelines created by intelligence managers.

At the core of the Kent approach is a grand bargain between policy makers and intelligence professionals. The intelligence community is master of its own house, but analysts and intelligence managers must avoid becoming embroiled in political decisions or commenting publicly or even privately on current policy or political issues. This division of responsibility is especially important because it gives intelligence analysts a special cachet in the U.S. political system, where the intelligence community is often seen as an objective source of information that is beyond the reach of partisan influence. Intelligence professionals take this bargain seriously. The organizational culture of the Central Intelligence Agency (CIA), for instance, reinforces this bargain through formal and informal norms and rules against political or policy commentary in the products produced by the Agency. Finished intelligence analysis also is scrubbed clean of policy content or obvious political bias that might have inadvertently crept into the work of analysts.

The strength of Kent's approach is that it preserves the independence of analysts by separating the intelligence community from the overt pressure or organizational and interpersonal incentives that can shape intelligence to conform to current policy or the personal and political biases of policy makers. Yet, by creating a strong barrier against politicization, Kent's prescriptions can separate intelligence too completely from policy makers, leading to other problems. For instance, policy makers are "inbox driven": They only have the time and energy to deal with their areas of responsibility or issues of immediate importance. Thus, weighty research papers offering reviews of broad issue areas or regions are likely to be ignored by policy makers. Those who are not responsible for the issues or regions covered will not read the paper, while those with a professional interest in the topic will seek more detailed analyses. Similarly, in-depth reports are likely to be ignored by most policy makers who have no responsibility for the issue surveyed. Without a good understanding of the issues that preoccupy specific policy makers, high-quality finished intelligence might be viewed as useless by intelligence consumers because it covers the wrong topics, arrives too late to be of use, lacks the proper level of detail, or addresses the wrong facet of the problem

at hand. In fact, without some sort of collaboration between analysts and policy makers, the arrival of timely, relevant, and useful finished intelligence would depend on luck.

Organizational pathologies also can emerge if intelligence managers and analysts become too detached from the needs of policy makers. Analysis can take on a life of its own as the personal or bureaucratic agendas of intelligence professionals begin to take precedence over the needs of their consumers. For instance, critics charged that the CIA's Office of Soviet Analysis (SOVA), especially its division specializing in the study of the Soviet economy, became increasingly scholastic as the Cold War progressed. Because the command economies of the Communist bloc had little in common with those of the capitalist West, the CIA was forced to create an entirely new academic discipline to understand Soviet economic performance and capability.[3] Promising academics were recruited from the best graduate schools and given specialized training, journals were founded to cultivate new methodologies and to provide a forum for theoretical debate, and analysts worked hard to gain insights into Soviet economic performance, a state secret of the Communist regime in Moscow. As analysts sought to sharpen their methodological skills and improve the sophistication of their theories, however, they began to lose sight of the big picture, especially the fundamental question that suggested itself to policy makers in the early 1980s. Could the Soviet command economy compete over the short term with the capitalist economies of the West, or was the regime in Moscow built upon an economic house of cards?

Actionable Intelligence

When Robert Gates, then Deputy Director for Analysis at the CIA, became frustrated with the unwillingness of CIA analysts to provide intelligence to meet the specific requirements of administration officials, actionable intelligence was born. Under Gates's system, analysts might have been asked, for example, when—not if—the Soviet economy would collapse. Intelligence professionals cried foul, noting that by posing specific and pointed questions, Gates was attempting to shape the analysis to suit the expectations of policy makers. In response, Gates suggested that he was trying to make analysts less academic so that they would produce relevant and timely finished intelligence that responded to the needs of administration officials.

The core assumption behind actionable intelligence is that analysts must be aware of the needs of policy makers and that intelligence managers have an obligation to task analysts so that they produce useful intelligence for their clientele. According to Gates:

> My view has been all along from the very beginning of my career—and perhaps due to the fact that I have served on the National Security Council—that the Intelligence community has to be right next to the policymaker, that [the analyst] has to be at his

> elbow—that he has to understand what is on his mind. He has to understand what his future concerns are. He has to understand what his agenda is. He has to understand some of the initiatives that he is thinking about taking. He has to be willing to ask the policymaker what he's working on, or what came of his last conversation with a world leader so that the intelligence can be made relevant; so that the Director, or the office director, or what can go back and give guidance to the analysts.[4]

From this perspective, policy makers already have a reasonable idea of what they need—information to help them implement their policies. Most of the support they require from the intelligence community is largely technical in nature: demographic, geographic, political, economic, and military data about the issue at hand and how allies and adversaries are responding to U.S. policies. Some observers have even noted that as crises emerge, policy makers should communicate with analysts directly to increase the flow of information and the timeliness of analysis. Under these circumstances, analytic debates within the intelligence community are counterproductive and actually reduce the confidence policy makers have in finished intelligence. When the chips are down, officials want information they can use to solve problems, not competitive analysis designed to highlight various theoretical or methodological approaches to the issues of the day.[5] In fact, some policy makers have discovered that the intelligence community can actually serve as an extension of their office staff, providing a ready source of analysis and information tailored to meet their personal interests and agendas.[6]

In reality, much of the finished intelligence produced by analysts takes the form of actionable intelligence: The information supplied to policy makers often is matter-of-fact data about what is occurring in a specific part of the world, the state of a foreign economy or industry, or the capability of a weapons system. Moreover, elected officials usually enter office with a pre-existing worldview and policy agenda; they look to the intelligence community to help them implement their policies. If intelligence professionals fail to recognize this political and policy reality, they risk becoming irrelevant.

Nevertheless, following the Gates model too closely can create its own set of problems. There is a possibility that policy makers will pose biased questions to the intelligence community to guarantee that analysis favorable to their positions will emerge, or that they will fail to pose the correct questions, leading to an incomplete understanding of the challenges they face. If analysts also concentrated only on actionable intelligence, they might lack the time to conduct the independent, in-depth research needed to uncover threats and trends not on current policy agendas. When they initially took office, for instance, members of the Bush administration had not placed Al Qaeda on the top of their foreign and defense policy agendas. Instead, they were more concerned with improving Russian-American relations, deploying a U.S. missile defense system, and reducing U.S military commitments overseas. It was up to the intelligence community to increase the salience of the terrorist threat to the United States among senior officials.

Normative theory and practice thus highlight the competing priorities that animate the intelligence-policy nexus. Analysts need some leeway, unconstrained by the preference of policy makers or even intelligence managers, to pursue their hunches and interests, regardless of current political or policy preferences. Without this freedom, policy makers would lack independent information and insight into current and emerging international issues. For their analysis to be relevant and timely, however, intelligence professionals must possess a keen awareness of policy makers' current interests and responsibilities. What policy makers require is information and finished intelligence reports that address the issues found in their inboxes. They also would benefit from long-term research that highlights emerging problems before they become crises or sources of embarrassment.

POLITICIZATION

Politicization, the effort of policy makers to shape intelligence to conform to their policy or political preferences, can emerge in both overt and subtle ways. Although the term suggests that intelligence analysts are victims when policy makers manipulate intelligence to suit their needs, intelligence professionals can themselves politicize intelligence when they allow bureaucratic or personal incentives to influence their estimates and reports. Intelligence managers and analysts can "pander" to policy makers by presenting them with information and analysis that meets their expectations and confirms their chosen policies. Intelligence estimates also can appear to be politicized when they are effective, that is, when they actually have a policy or political impact.

Overt politicization occurs when policy makers deliberately pressure analysts to produce estimates that support their policies or to shape the intelligence cycle to confirm current policy or political preferences. The act of deliberately shaping intelligence estimates would have to be driven by expediency or desperation because policy makers run a grave risk by preventing accurate, if unpleasant, information and finished intelligence from informing national policy. In extreme cases of politicization, senior officers or policy makers can even retaliate against analysts for providing them with information that contradicts their existing beliefs or plans. In the days leading up to Operation Market Garden, the Allied airborne-armor operation to seize the Rhine River crossings in September 1944, Major Brian Urquhart, Chief of Intelligence for the British I Airborne Corps, detected signs that Nazi armored divisions were actually bivouacked in Arnhem, that last objective of the Allied advance. When Urquhart relayed to his superiors this information, which called into question the feasibility of the entire operation, he was visited by a senior medical officer who placed him on sick leave.[7]

Overt politicization, however, is difficult to keep concealed, because analysts and intelligence managers will go to great lengths to resist what they believe are illegitimate efforts to influence their finished intelligence reports. In the aftermath

of the Vietnam War, for instance, Samuel Adams, a former CIA analyst who helped develop estimates of enemy troop strength during the war, charged that senior intelligence officials and military officers deliberately suppressed his findings because they gave the Viet Cong greater strength than had been reported in previous intelligence estimates. The controversy over the incident only increased in the aftermath of the conflict, and became the subject of a CBS news documentary and libel litigation between General William C. Westmoreland (retired), who was the former head of the Military Assistance Command in Vietnam, and CBS.[8] Some controversies boil over even more quickly. Following the second Gulf War, accusations emerged that the members of the George W. Bush administration had tried to undermine the credibility of Ambassador Joseph Wilson, who investigated reports that Iraqi agents had attempted to purchase yellowcake, a nuclear material, from Niger. Wilson had turned in a memo to intelligence officials in February 2002, explaining why the alleged Iraqi activity was probably a hoax. When the president claimed in his 2003 State of the Union Address that Iraq had sought uranium in Africa, Wilson went public in a July 6, 2003, editorial in the *New York Times,* stating that the Bush administration knowingly lied about the status of Iraq's nuclear program. In retaliation, Bush administration officials allegedly "outed" Valerie Plame, Wilson's wife, effectively ending her career as a clandestine CIA officer.[9]

Although they make headlines, charges that policy makers deliberately engage in politicization are relatively rare. Instead, policy makers and intelligence managers can shape analysis in more subtle, and sometimes even inadvertent, ways. Those who bring positive news can be rewarded with praise in front of colleagues, whereas those who bring unwelcome information can be chastised or criticized in front of their coworkers. "Positive" estimates are more likely to be rewarded with promotions, increases in pay, or sublime inducements important to bureaucrats—a larger office, new furniture, travel. "Negative" estimates are unlikely to be rewarded; in fact those with an eye for finding potential trouble in a generally positive situation are often avoided by policy makers whose workday is often spent responding to a never-ending series of crises, problems, or complaints. Loss of access to policy makers can take the form of *bureaucratic death*, a situation in which intelligence officials are no longer invited to important meetings because of their history of providing contradictory or discouraging reports.[10] Only the smartest and toughest policy makers encourage their staffs to take steps to avoid sending inadvertent signals to subordinates and intelligence mangers to prevent analysis from being shaped to meet their expectations or to emphasize the positive aspects of every situation. Indeed, some observers have noted that the ability to literally pressure subordinates to provide honest assessments is a key to success in politics and war.[11]

Without knowing it, however, efforts to encourage analysts to provide their honest opinion can have unintended consequences. During the Vietnam War, for example, General Westmoreland was provided with a negative assessment of his command's ability to hold the marine position at Khe Sanh, the findings of an

estimate that he had personally requested. After hearing the report, which was delivered to his entire staff, he thanked the analysts for their best estimate and then stated that he would no longer tolerate gloomy evaluation of the marine's prospects at Khe Sanh. Years later, Westmoreland's chief of intelligence, Major General Philip Davidson (retired) remarked that he had never heard a negative prediction for the outcome at Khe Sanh. In what was an apparent effort to bolster morale, Westmoreland had told his command that he no longer wanted negative reports about the situation at Khe Sanh. It is not surprising that his staff complied.[12]

When intelligence has an effect on important foreign and defense policy debates, charges of politicization often emerge. Ironically, when intelligence analysts offer timely and relevant estimates to policy makers, they are sometimes accused of meddling in political affairs because their reports have an impact, favoring one side in a political dispute over another. As issues become increasingly a matter of heated partisan politics or less focused on technical issues, the role played by intelligence analysts as neutral purveyors of information and analysis increases. Moreover, if the finished intelligence in question was not backed by a clear analytical consensus, there always will be intelligence "dissenters" ready to take their case to elected officials or the media. As Richard Betts has noted, this is exactly the situation that emerged in the controversy over enemy strength during the Vietnam War: The effort to shape an analytical consensus spilled over into acrimony that lasted for years and became a matter of public and political debate.[13]

THE INFORMATION REVOLUTION AND THE INTELLIGENCE POLICY NEXUS

The information revolution has broken down barriers of space and time by virtually eliminating the costs of communication, even at intercontinental distances. The computer and the Internet have provided individuals with an ability to organize and analyze information that was unheard of only a few decades ago. The Internet itself is a positive-sum institution: The more people who have access to the Internet and this virtually free means of communication, the more powerful the tool becomes for all concerned.[14] The real power of new computing and communication architectures is that they can potentially allow people everywhere and anywhere to find and interact with each other in real time.

As with any technology, the information revolution contains its own embedded ideology, so to speak: People will find that it should be employed in a particular way, regardless of the intentions of its designers. In fact, the inventor of a machine is often unaware of the logic inherent in the technology he or she is creating. Gutenberg was a Catholic, but his printing press made the Protestant reformation possible because printing facilitated the dissemination of competing ideas (i.e., heresy).[15] The automobile transformed America—dispersing extended families and building suburbs and new American cultures.[16] The automobile's

effects, however, were perceived only when the transformation of society was well under way.

The information revolution also is transforming society. It is an egalitarian technology that breaks down social, economic, political, and bureaucratic barriers and allows people direct access to each other's very personal "inboxes," for the most part facilitating frank communication even across hierarchical organizations. At the same time, the information revolution also documents human interaction as it channels not just formal, but informal, communication into what amounts to official or corporate records. In a sense, people have to convert private interactions into a public record to participate in the information revolution, but they seem to accept this as the price of entry for using the new technology.

Because we use information revolution technologies on a daily basis, we often overlook the subtle and even not so subtle changes it is bringing to everyday life or well-understood bureaucratic practices. In terms of the intelligence-policy nexus, for example, the information revolution has reframed the opportunities for interaction between intelligence analysts and policy makers in ways that are not well captured by either the Gates or Kent frameworks. The barriers to interaction assumed by the Kent model, which are supplied by intelligence managers or by the process of crafting formal intelligence estimates, are completely broken down by the information revolution. Policy makers and their staffs can now easily communicate on a daily basis directly with analysts. It is increasingly difficult for analysts to stand above the fray of politics or policy if they are bombarded with a barrage of questions about current policy, calls for data, or requests for commentary or supplemental information about media coverage of some international event. Moreover, as the volume of this informal interaction between policy makers and analysts increases, it can begin to drown out the message carried by the formal estimates offered by intelligence organizations. Because of the sheer volume of interaction between analysts and policy makers, it also might be nearly impossible for intelligence managers to monitor this informal communication, and any effort to restrict analysts' access to this communication technology would be resisted on both personal and professional grounds. The information revolution has created a new medium for interaction between analysts and policy makers that, by its very nature, flies in the face of the norms suggested by Kent's framework.

Policy makers' access to analysts is so great that it can overwhelm them, degrading their ability to provide significant actionable intelligence called for by the Gates model. It might be difficult for individuals outside of government or the military to understand, but as members of a "service industry," intelligence analysts must place the immediate needs of administration officials ahead of other important professional or organizational objectives. Questions or requests for information, no matter how trivial, must receive a prompt and complete response. Additionally, because service is part of the ethos of the intelligence community, performance metrics are focused on measuring responsiveness to policy makers' demands, not the quality or thoroughness of the response given or the opportunity costs created by setting aside long-term research projects. Because everyone

within the policy-making and intelligence communities is virtually free to task analysts, intelligence managers are no longer able to set production priorities or timelines. In fact, because managers are judged by the same production metric as analysts, they have little incentive to intervene in informal communications to protect analysts from being endlessly besieged with questions by policy makers.

The information revolution offers more opportunities for intelligence analysts to interact with officials while making it increasingly difficult for analysts to hold their attention. Because policy makers have ready access to nongovernmental sources of information provided by twenty-four-hour cable television and Internet news services, intelligence analysts have to hold the attention of policy makers by providing catchy titles to reports that exaggerate the importance or the certainty underlying estimates. The Silberman-Robb Commission, which investigated the intelligence community's account of Iraq's weapons of mass destruction program prior to the second Gulf War, found that the *President's Daily Brief* (PDB)—a tightlyheld piece of finished intelligence that is read by a few select senior officials on a daily basis—suffered from various flaws and created several problems.[17] PDBs tended to contain bold statements and judgments that were probably intended to engage the reader but failed to convey a sense of the qualifications, judgments, or assumptions that were embedded in the analysis. Commissioners were concerned that a daily exposure to PDB briefings might "create, over time, a greater perception of certainty about their judgments than is warranted." Questions posed to PDB briefers are answered in future PDBs or in a Senior Executive Memorandum, which are distributed to all those who receive the PDB. Commissioners believed that the volume of reporting that could be produced by a question of clarification, for example, could create a false impression among PDB recipients that the president was intensely interested in a subject, thereby shaping priorities and policy.[18]

The commissioners also searched in vain for evidence of politicization in the intelligence community's reporting on Iraqi weapons of mass destruction programs. What they uncovered, however, was evidence of the impact of the information revolution—especially the breakdown of hierarchy. The CIA Ombudsman for Politicization told the commissioners, for example, that analysts on Iraqi issues worked under more "pressure" than any other analysts in the history of the CIA. For months they were required to provide enormous amounts of both formal and informal reporting directly to the highest officials in the U.S. government. These officials also questioned analysts directly about their work to explore the assumptions and data that were used. Policy makers are justified in asking these types of questions, regardless of their motivations, but the fact that senior officials apparently scrutinized analysts directly probably affected subsequent analysis. Analysts also were under pressure "to answer the mail quickly," which in itself can be detrimental to calm contemplation of complicated issues.[19] Cutting and pasting is not a measured reassessment of first principles or even secondary assumptions, and it unfortunately occurs when timeliness takes precedence over depth in the information age.

CONCLUSION

Intelligence reform is cyclical. Sometimes scholars and other observers warn that analysts are too detached from policy makers' concerns and are producing finished intelligence that is dated or irrelevant. At other times, concerns about politicization emerge; observers worry that intelligence analysts and managers are no longer serving as an independent source of information for policy makers and that the intelligence cycle has been corrupted by all sorts of political or bureaucratic considerations. Since the early 1980s, the pendulum has been swinging in favor of producing "actionable" intelligence, but in the aftermath of a series of intelligence setbacks leading up to and following the September 11, 2001, terror attacks, observers have had second thoughts about the status of the U.S. intelligence community. Intelligence reform, based on organizational change, is the order of the day.

It is extraordinarily difficult to strike a balance between detachment and responsiveness in the intelligence-policy nexus. As Betts noted, fixing one type of intelligence problem only exacerbates other types of problems.[20] For instance, providing all available information to analysts would overwhelm them; by contrast, restricting the flow of information creates the risk that they will not receive critical bits of information needed to make sense of emerging threats. Because the correct balance of detachment and responsiveness depends upon the specific issue or problem confronting intelligence analysts and policy makers, it is virtually impossible ex ante to fine-tune the intelligence-policy nexus.

In a sense, those interested in intelligence reform are addressing a moving target. The proper balance in the relationship between intelligence professionals and policy makers is shaped by external and internal factors. Externally, the changing threat environment and issue agenda create different types of challenges for the intelligence community. Reporting on developments within nation states requires different collection and analytical capabilities than does reporting on terrorist networks or superempowered individuals. Internally, new communication and information processing capabilities—combined with the way analysts and policy makers actually use these novel capabilities—are creating new modes of interaction within the intelligence-policy nexus. It might be too early to sound the death knell for the Kent and Gates models, but in the future it will probably become increasingly difficult to capture the reality of the intelligence-policy nexus within these competing theoretical frameworks.

NOTES

1. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press, 1946).

2. H. Bradford Westerfield, "Inside Ivory Bunkers: CIA Analysts Resist Mangers' 'Pandering'—Part II," *International Journal of Intelligence and Counterintelligence* 10 (Spring 1997), pp. 19–54; Richard K. Betts, "Politicization of Intelligence: Costs and

Benefits," *Paradoxes of Strategic Intelligence,* eds. Richard K. Betts and Thomas Mahnken (London: Frank Cass, 2003), pp. 59–79.

3. David M. Kennedy, *Sunshine and Shadow: The CIA and the Soviet Economy* (Cambridge: Harvard University, JFK Case Program, 1991).

4. Gates quoted in Westerfield, "Inside Ivory Bunkers."

5. William Odom, *Fixing Intelligence: For a More Secure America* (New Haven, CT: Yale University Press, 2003).

6. Jack Davis, "A Policymaker's Perspective on Intelligence Analysis," *Studies in Intelligence* 39 (1995), pp. 7–15.

7. Sir Brian Urquhart, who was Under-Secretary-General of the United Nations (UN) from 1974 to 1986, played a leading part in the development of UN peacekeeping operations throughout the Cold War. Urquhart was eventually knighted for his service to the United Nations.

8. James J. Wirtz, "Intelligence to Please? The Order of Battle Controversy During the Vietnam War," *Political Science Quarterly* 106 (Summer 1991), pp. 239–63.

9. "Then & Now: Joseph Wilson," CNN, 19 June 2005, available at http:// www.cnn.com/2005/US/03/07/CNN25.tan.wilson/index.html.

10. Mark Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: CQ Press, 2003), p. 148.

11. Eliot Cohen, *Supreme Command* (New York: Free Press, 2002).

12. Phillip Davidson, Interview II by Ted Gittinger, June 30, 1982, Oral History Collection, LBJ Library, Austin, Texas, pp. 23–24; and William C. Westmoreland, *A Soldier Reports* (Garden City, NY: Doubleday, 1976), p. 338.

13. Betts, pp. 73–74.

14. Bill Gates, *The Road Ahead* (New York: Penguin, 1996).

15. Printing increased literacy because it provided common people with something to read. Without printing, Martin Luther could not have encouraged people to read the Bible themselves.

16. George F. Kennan, *Around the Cragged Hill* (New York: W.W. Norton, 1994).

17. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, "Report to the President of the United States," 31 March 2005.

18. Ibid., pp. 160–81.

19. Ibid., pp. 187–89.

20. Richard Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics*, 21 (October 1968), pp. 61–89.

9

SORTING THE WOOD FROM THE TREES

Were 9/11 and Iraq "Intelligence Failures"?

PETER GILL

THE SEPTEMBER 11, 2001, ATTACKS ON New York and Washington (9/11) and, then, the lack of the predicted weapons of mass destruction (WMD) in Iraq apparently represent two highly significant intelligence "failures," especially in the United States, with the best-endowed intelligence community in the world but also, in the case of Iraq, for the United Kingdom.

If journalists provide the first draft of history and, sometimes, official inquiries provide the second, then it falls to academics to provide a third. This is distinguished from the first two, in part, by facing fewer deadlines but also, it is to be hoped, by providing a broader context for analysis rooted in the previous literature of the subject. Journalists will probably not have the time and may not have the expertise to do this, and the objective of governmental inquiries is determined largely by their timescale and terms of reference. Congress has investigated both 9/11 and Iraq, as have special commissions,[1] and in the United Kingdom aspects of the Iraq WMD issue have been investigated by various parliamentary, judicial, and special inquiries.[2]

This chapter places 9/11 and Iraq in a broader context of the literature on previous intelligence failures in order to answer some key questions:

- What do we mean when we talk of intelligence failure?
- To the extent that these were failures, what caused them?
- Were they, in fact, political as well as intelligence failures?

WHAT IS INTELLIGENCE FAILURE?

The fact that there are clear limits to intelligence is easily demonstrated by reference to a few of the defining events of the last century that U.S. and other intelligence services failed to anticipate. Any such list would have to include failures to predict the Soviet testing of its first atomic bomb, the North Korean invasion of South Korea, the construction of the Berlin Wall, an apparent string of failures over Vietnam, the Soviet invasion of Czechoslovakia in 1968 and of Afghanistan in 1979, the Iranian revolution of the same year, the Polish crisis of 1980–81 and, more centrally, given that its primary focus for over forty years was the USSR, the end of the Cold War.

In much of the literature the implicit or explicit assumption is that intelligence exists to inform policy. With specific respect to national security threats, states gather information at home and abroad, establish structures for its analysis, and then disseminate the resulting intelligence to those in executive or policy-making positions for them to act on. The role of intelligence is, therefore, as a servant of power—it should, where possible, speak truth unto power so that politicians do not act based on misunderstandings of their position. Intelligence tells it like it is, and if the politicians do not like it, then that is their problem (and ours).

It follows that a "failure" occurs when intelligence gets it wrong so that misleading information is presented to executives resulting, possibly but not inevitably, in unsuccessful policy. (Intelligence may be wrong but superior power may nevertheless enable an adversary to be overcome.) Although failures may occur on different timescales, there are essentially two types: false negatives and false positives. In the first, there is a failure to apprehend something that is a threat, with the result that a surprise attack is suffered; in the second, a threat is perceived but turns out to be baseless. Clearly, 9/11 in the United States (and July 7, 2005, in the United Kingdom) represent the first type, and the misapprehension of Iraqi WMD represents the second. Although there may be common factors in the explanation of these different types of failure, it is important to bear in mind that there are also key differences.

We need to be careful as to how we delineate failure. It is the thankless task of intelligence to seek to prevent nasty surprises—sometimes very nasty ones—but we have to maintain a sense of the realistic. It is simply not feasible to construct a security intelligence process that can guarantee freedom from surprise attacks. George Orwell imagined how such a society would look in his novel *1984*. There, a Hobbesian state was able via total surveillance to guarantee internal security to its citizens but only at the cost that the state itself constituted a major threat to citizens' security. It only makes sense to judge failure in the context of what we might reasonably expect security agencies to know, given their size, resources, etc. But though the sheer diversity and complexity of the world from which threats emanate ensure that surprises will always remain a possibility, surely we should be able to organize better to ensure that "type 2" failures do not occur. For example, these are less urgent: If there is no actual attack (because there is, in

reality, no threat), then there will be more time for analysis (though anxious politicians may not perceive things that way). Indeed, the new doctrine of "preventive" war enunciated in Washington and London since 9/11 actually increases the importance of security intelligence because it must provide the basis not just for policy but also for the public justification for that policy.

But there is another complication, as evidenced in the Iraqi failure. It was stated above that intelligence exists to inform policy, yet this formal, textbook relationship may not pertain in the messy world of government. Governing politicians and other executives tend not to sit idly by while intelligence officials contemplate the nuances of their analyses—they desire to act and, given their survival skills, often believe that their own information, contacts, senses, and judgments are at least as good as those of officials. Consequently, their policies are as likely to be informed by their own beliefs, ideologies, and perceptions as they are by official intelligence reports. This is not always a problem, because the inclinations of governing officials and politicians will often be more or less in step anyway, but, on occasion, they may be significantly different and then there may well be problems.

To put this more conceptually, the crucial relationship between intelligence and policy is a subset of the more general relationship between information and power: any individual, organization, or government seeks information in order to inform better its actions, including attempts to exert influence or power. However, this "rational actor" model is more of an ideal type than an actual description of what happens in the world. We may well find that the relationship between information and power is reversed, so that what our actor actually determines to be relevant information depends on what he or she wants to do or how he or she wants to do it. In life and government, not only does what you see depend on where you sit (a matter of perception) but also on what you want to do (a matter of power). Thus, at whatever level of power and decision making we are interested—individual, group, corporate, governmental—people may not only pay more attention to information that tends to support their preferred position but actually discredit anything that contradicts it as mischievous or deception.

So, in the cases of 9/11 and Iraq we can identify three main possibilities: they were examples of intelligence failure, in which the professionals in the relevant agencies failed to generate sufficient information and/or analyze it correctly so that their governments were misinformed; they were examples of political failure, in which governments' actions or inactions were based on pre-existing beliefs, judgments, or ideologies and the role for intelligence was to provide post hoc rationalization for those decisions in order to sell them to sceptical publics; or, these cases represent a messy mixture of both professional and political failures.

WHAT CAUSES INTELLIGENCE FAILURE?

Michael Herman identifies two general conclusions from a survey of the literature: first, the weak link is not so much a failure to collect information as to

analyze it and, second, the weakness is intellectual rather than administrative: "People interpret data through images, historical analogies, personal experiences and other hypotheses. There is a cognitive rigidity about the way they fit information into these patterns. They see what they expect to see; they come to conclusions too early and stick to them for too long."[3] There was a direct echo to this in the conclusion of the 9/11 Commission that one of the main contributory factors was a failure of imagination.[4]

Fundamental are the problems of overload and complexity. The very sophistication of modern information-gathering systems produces the problem of overload. Intelligence systems may demand ever more data in the empirical illusion that more data will solve the mysteries and secrets when, in fact, they are likely to suffer the fate of the thirsty individual who tries to drink from a firehose. As the 9/11 Report noted: "One can see how hard it is for the intelligence community to assemble enough of the puzzle pieces gathered by different agencies to make some sense of them. . . . Accomplishing all this is especially difficult in a transnational case. We sympathize with the working-level officers, drowning in information and trying to decide what is important."[5]

Overload manifests itself also in the concept of "noise," wherein the glut of extraneous material inhibits the analyst from focusing on the information that is central to the analytical problem or even prevents the analyst from spotting it.[6] Despite the problems of overload, of course, it may well be that the information system just does not contain the information that it needs in order to develop the required intelligence. In order to deal with overload, all systems must select information as being relevant to the purpose for which it is required, but if the methodology for selection is misguided or outdated, relevant information may be missed. The less an agency or analyst knows about a problem, the greater the danger of overload; in contrast, experts in their fields may be the most likely to cling to longstanding interpretations in the face of anomalous information—the "paradox of expertise."[7] One way of reducing complexity is to narrow the focus of analysis. However, the more this is done, the more there is a risk of error as a result of oversimplification. One possible reaction to the difficulties of analyzing other societies and cultures is *mirror-imaging*: assuming, simplistically, that they operate much like one's own.[8]

Further, these intellectual shortcomings may be compounded by internal administrative obstacles; these have been variously characterized in the literature as distortions[9] or pathologies.[10] Specialization is a key feature of the Weberian bureaucracy and serves many useful purposes, but maximizing the efficiency of information flows and encouraging imagination are not prominent among them. In intelligence bureaucracies there are additional hurdles that, again, may be soundly based, but further hinder the flow—notably secrecy and compartmentalization of information.[11] This may occur both within and between organizations: for example, analysts may be in complete ignorance of information that would be important for their work because they are perceived not to "need to know" aspects of specific operations. This may be compounded by the existence

of different databases; if they cannot be linked, the information is effectively hidden from analysts. The 9/11 Commission showed how, given the poor state of the Federal Bueau of Investigation's (FBI) information systems, analysts' ability to access information depended largely on whether they had a personal relationship with anyone in the squad where the information resided.

Given these findings, it is ironic that such large sums of money have been poured into the development of ever more sophisticated technical systems for the *collection* of information compared with the miniscule expenditure on *analysis*:

> The FBI's information systems were woefully inadequate. The FBI lacked the ability to know what it knew: there was no effective mechanism for capturing or sharing its institutional knowledge. FBI agents did create records of interviews and other investigative efforts, but there were no reports officers to condense the information into meaningful intelligence that could be retrieved and disseminated.[12]

The modern transformation of intelligence by the application of highly sophisticated surveillance and information technology has overshadowed the fact that, at its core, it remains an intellectual process. Technology can contribute to analysis. For example, since 9/11 there has been great emphasis on developing relational software to "mine" disparate data sets gathered in "data warehouses," but the attribution of meaning to items of information or linked items requires the application of thought and judgment. However many facts are compiled or integrated, they still do not speak for themselves and analysis requires the testing out of different possible explanations against the evidence.

Finally, in addition to cognitive and bureaucratic obstacles to analysis, we must remember that those states, organizations, groups, or people who are the targets of intelligence operations are unlikely to remain passive. They have their own objectives and deploy their own techniques to counter attempts to discover their secrets. These may be just defensive but may also attempt to deliberately mislead and thus disrupt an opponent's operations. Therefore, as analysts seek to manage overload and complexity, they must not forget that some of the information they obtain may be intended to mislead them. As we shall see, this was a factor in the Iraq debacle.

COLLECTION AND ANALYTICAL FAILURES ON IRAQ

The issue of the absent WMD in Iraq has become the most investigated failure of all time. In the United States both the Senate Select Committee and the Silberman-Robb Commission have reported, in the United Kingdom no fewer than four inquiries have taken place, and Australia had two. Surely, therefore, we have the definitive picture of what went wrong. Well, arguably, no. Certainly, the combined output of these inquiries has provided enough raw materials for a

future avalanche of scholarly discussions of intelligence failure because they picked over in minute detail the performance of the professionals but, by comparison, they skirted around the issue of policy or political failure.[13]

The U.S. Senate Select Committee on Intelligence (SSCI) inquiry into the U.S. intelligence community's prewar intelligence assessments on Iraq, beginning in June 2003, set out to consider the quantity and quality of U.S. intelligence on Iraqi weapons of mass destruction programs and ties to terrorist groups; "the objectivity, reasonableness, independence, and accuracy of the judgments reached"; whether these were properly disseminated to the executive and legislative branches; and whether any political pressure affected these assessments.[14] In February 2004, the committee announced that the second phase of its report would appear only after the 2004 presidential election. This would cover the more politically contentious issues of the extent to which, if at all, government statements had exaggerated the intelligence. But, in the event, it was not produced.

The overall SSCI conclusion on the national intelligence estimate (NIE) on Iraqi WMD produced quickly in October 2002 is damning. "Most of the major key judgments," it concluded, were "either overstated, or were not supported by, the underlying intelligence reporting. A series of failures, particularly in analytic trade craft, led to the mischaracterization of the intelligence."[15] The failure is firmly located as being overwhelmingly one of analysis, with some failures in collection, all compounded by poor management and an environment that seemed to militate against information sharing.[16] In short, the report assigns responsibility for the failure first to analysts, second to managers and bureaucratic structures, and third to failures in collection.

On collection, the SSCI criticized the heavy reliance during the 1991–98 period on United Nations Special Commission (UNSCOM) inspectors and the fact that the intelligence community did not use the period of the inspections to establish human intelligence (HUMINT) sources that could replace the inspectors in the event of their departure. Incredibly, in light of the certainty of the conclusions contained in the October 2002 NIE, after 1998 the intelligence community did not have any HUMINT source of its own reporting on Iraqi WMD.[17] Similarly, none of the United Kingdom's human sources was able to report directly on WMD.[18] Interestingly, given the amount of money expended on it, there is very little comment in the SSCI Report and none at all in Butler on the absence of any signals intelligence (SIGINT) regarding WMD.

The SSCI found that the assessment that Iraq "is reconstituting its nuclear program" was not supported by information that dual-use equipment was being purchased because it failed to show that it was destined for an Iraqi nuclear program. As with the British government's September 2002 dossier, judgments that Iraq "has chemical and biological weapons" overstated conclusions that could be safely reached on the basis of the available intelligence.[19] On chemical and biological weapons (CBW), suspicions based on Iraq's past technological capabilities in this area, deception practiced against UNSCOM, and past failure to satisfactorily account for all CBW holdings and precursors could have supported

a conclusion that Iraq may have had such weapons, but the leap to asserting that it actually had them was not justified by the raw information.

The claim that Iraq was "vigorously trying to procure uranium ore and yellowcake" via Niger exaggerated the existing state of knowledge.[20] Moreover, once it emerged that claims as to Iraqi attempts to procure material via Niger were based on forged documents, both the CIA and the Defense Intelligence Agency (DIA), "continued to publish assessments that Iraq may have been seeking uranium from Africa," and the CIA "continued to approve the use of similar language in Administration publications and speeches, including the State of the Union."[21] In the United Kingdom, Butler concluded that there was evidence that Iraq had sought uranium from Africa although there was no evidence that it had obtained any.[22]

Analytically, the failure was explained by "groupthink," a risk inherent in organized intelligence analysis, and one also identified as a source of the intelligence failure that occurred in the United Kingdom and Australia. In this case it manifested itself in the dominant assumption that Iraq possessed and was concealing WMD, and that "led Intelligence Community analysts, collectors and managers to both interpret ambiguous evidence as conclusively indicative of a WMD program as well as ignore or minimize evidence that Iraq did not have active and expanding weapons of mass destruction programs."[23] We should also note the significance of evaluating the absence of information: "Absence of evidence may not be evidence of absence" but no more should it be taken as "evidence of presence" as it was too often in the case of Iraq.

One important factor in this response was the failure a decade earlier to identify the active nuclear weapons program that did then exist in Iraq and that was destroyed after 1991. Similarly, the U.K. Butler inquiry concluded that there was a "tendency for assessments to be coloured by over-reaction to previous errors."[24] The then-recent avalanche of criticism at the agencies' failure to prevent 9/11 was another. So strong was this dynamic, according to the SSCI, that managers shared the same groupthink presumptions and so did not utilize established mechanisms to challenge them. "Red teams" or "devil's advocate" approaches were simply not used in this case. The report concluded that managers, "did not encourage analysts to challenge their assumptions, fully consider alternative arguments, accurately characterize the intelligence reporting, or counsel analysts who lost their objectivity."[25]

Excessive compartmentalization of HUMINT regarded as sensitive was identified as a factor inhibiting the production of the most effective analysis. The committee concluded that the process by which the intelligence community "calculates the benefits and risks of sharing sensitive human intelligence is skewed too heavily toward withholding information."[26] However, the committee found that the problem of information sharing went further, and that there was a tendency for the CIA to deny information to more specialist agencies that could have allowed for input that challenged existing presumptions.[27] Known dissenting views from other parts of the intelligence community were not always included in assessments where they would have challenged the dominant

assumption—as, for example, over the debate concerning the purpose of aluminum tubes. In some cases assessments that conformed to the dominant assumption bypassed specialist agencies that were in a position to challenge them.[28] The U.K. Butler report made precisely the same criticism.[29]

The Silberman-Robb commission, set up by the president to explore the reasons for the intelligence failure over Iraq's WMD, reinforced the conclusions of the SSCI. But analysts were central once again. At some point, they concluded, analysts' assumptions about Iraqi WMD:

> stopped being working hypotheses and became more or less unrebuttable conclusions; worse, the intelligence system became too willing to find confirmations of them in evidence that should have been recognized at the time to be of dubious reliability. Collectors and analysts too readily accepted any evidence that supported their theory that Iraq had stockpiles and was developing weapons programs, and they explained away or simply disregarded evidence that pointed in the other direction.[30]

As Michael Herman noted, no one was asking the question: "Could it be because there are no WMD at all?"[31] But if anyone thought so, "no one wanted to say that because so much intelligence would have to be discounted."[32]

FAILURE TO DISSEMINATE INTELLIGENCE

If the attention and resources devoted to analysis have paled in comparison with that given to collection, the same may be said of dissemination. Again, this can contribute to failure because, at the risk of stating the blindingly obvious, if intelligence is not communicated to someone who can do something with it, the so-called intelligence process may be reduced to a self-serving cycle of collecting and storing information. Completed analyses may be disseminated in various forms, but there are problems of sharing. For example, analysts need to know the credibility of the sources of the information with which they are dealing, but handlers may be reluctant to admit their own doubts about their sources' veracity. Obstacles to sharing information with other agencies are even more extensive. This may reflect the choice of the agency not to share the information outside or simply a lack of awareness that anyone outside would be interested.

Much criticism after 9/11 in the United States concentrated on this failure to share information with others. In some cases this rightly aimed at failures to share based on nothing more than ignorance or poor understandings, but there are also understandable and defensible reasons. For example, all agencies jealously guard their sources and methods not just because they are short-sighted but also because they fear their compromise if information they provide is used unwisely. Recipients outside the community may not appreciate that the publication of an item of intelligence can enable a target to identify and eliminate its source—in some cases a person. Nevertheless, the 9/11 Commission described clearly the failures

of sharing information between U.S. agencies prior to the attacks[33] and recommended that the Cold War assumption that intelligence can only be shared with those who need to know must be replaced by a need-to-share culture of integration.[34]

Dissemination within the community is an important factor in the quality of final products, but it is dissemination outside of the community that establishes the credibility and utility of intelligence. The primary consumers of intelligence are the "doers"—political or corporate. How intelligence conclusions are presented is important: specifically, how does it present degrees of uncertainty? The use of language is crucial; indeed it is determinative of what, in the end, is considered to be the knowledge upon which policy may be based or by which it is rationalized. Intelligence seeks to improve knowledge by reducing uncertainty but is only ever partially successful. The way in which different national systems seek to convey this uncertainty varies. For example, U.S. NIE incorporate footnotes recording the dissents of particular agencies from the main conclusions and the CIA provides percentage probabilities of success in possible future operations.[35] The SSCI found that the language used throughout the NIE, "did not accurately portray the uncertainty of the information," and instead "portrayed what intelligence analysts thought and assessed as what they knew and failed to explain the large gaps in the information on which the assessments were based."[36] Policy makers were denied the context that open acknowledgment of the gaps in the intelligence picture would have provided. Moreover, where uncertainty was expressed (as was also the case in the United Kingdom and Australia), it was used to suggest that Iraq's WMD were even more extensive than indicated, but that clever Iraqi denial and deception techniques, refined throughout the period from 1991, had effectively concealed the scale. In the United Kingdom the Joint Intelligence Committee (JIC) eschewed dissenting footnotes and the Butler Review described how the JIC accommodated uncertainty. When the intelligence was unclear or inadequate, the JIC reported alternative interpretations as long as the membership agreed they were viable,[37] but minority hypotheses were not produced. So it normally attempted to reach a consensus in the assessment, and the section of Key Judgements would often include warnings as to the thinness of the evidence. Inevitably this search for consensus "may result in nuanced language. Subtleties such as 'the intelligence indicates' rather than 'the intelligence shows' may escape the untutored or busy reader. We also came across instances where Key Judgements unhelpfully omitted qualifications about the limitations of the intelligence which were elsewhere in the text."[38] But if language is nuanced in order to satisfy those who are producing it, the subtleties of what they mean may well escape those who receive it. If, as Butler noted, not even the producers are themselves clear as to the significance of the language, what hope is there for the reader?

> We have been told that some readers believe that important distinctions are intended between such phrases as "intelligence indicates . . .", "intelligence demonstrates . . ."

> and "intelligence shows . . .", or between "we assess that . . .", "we judge that . . ." and "we believe that . . .". We have also been told that there is in reality no established glossary, and that drafters and JIC members actually employ their natural language.[39]

Butler did not suggest any particular way of trying to deal better with this problem—it is indeed inherent in any process involving language—but recommended that the intelligence community review their conventions.[40] The government's response was that the guidance to staff on use of language had been reviewed and reissued (we might also hope that politicians are inducted into them) and that JIC minutes are now to include "alternative and minority hypotheses or uncertainties."[41]

In the broadest sense all intelligence provides warnings, but states and corporations alike view warnings of nasty surprises as the central intelligence function. During the Cold War sophisticated systems were developed for the surveillance of indicators that an attack might be pending. For example, during 1950–75 the United States had a watch committee and National Indications Center and Soviet military intelligence (GRU), and the KGB maintained similar systems for indications of Western attacks.[42] Now that the fear of attacks from non-state actors has replaced these, the process of providing appropriate indicators is much more difficult and the judgments to be made in issuing warnings are acute. The 9/11 Commission noted that, with the exception of the analysis of Al Qaeda attempts to obtain WMD, the U.S. intelligence community failed to apply warning methodologies to the potential threat of terrorist attack on the United States.[43]

And, yet, warnings there were: Chapter 8 of the 9/11 Commission report effectively conveys the same story that former Clinton and Bush administration terrorism coordinator Richard Clarke had already told of serial warnings but there was no policy response.[44] In part this reflected the still-dominant Cold War assumptions of the foreign policy experts upon whom the new president relied that threats came essentially from states. The key document in alerting the administration should have been a *President's Daily Brief* (PDB) from August 6, 2001, containing an item headed "Bin Laden Determined to Strike in U.S." It was the thirty-sixth PDB item relating to Bin Laden or Al Qaeda in 2001.[45] The analysts who produced the item were responding to an inquiry by the president about whether any threats to the United States existed, and to them "represented an opportunity to communicate their view that the threat of a Bin Laden attack in the United States remained both current and serious." The president told the inquiry that the report "was historical in nature" and that "if his advisers had told him there was a cell in the United States, they would have moved to take care of it." However, the PDB contained a number of potential warnings, including the fact that FBI information "indicates patterns of suspicious activity in this country consistent with preparations for hijackings or other types of attacks, including recent surveillance of federal buildings in New York."[46]

At the same time, analysts' fears about the possibility of an attack on the United States were not reaching the right people. The commission reported: "Most of the intelligence community recognized in the summer of 2001 that the number and severity of threat reports were unprecedented." However, despite the number of fragments, there were too few specifics to point to a named target. Moreover, the 9/11 planning fell into "the void between foreign and domestic threats," which made it harder to make sense of the fragments:

> The foreign intelligence agencies were watching overseas, alert to foreign threats to US interests there. The domestic agencies were waiting for evidence of a domestic threat from sleeper cells within the United States. No one was looking for a foreign threat to domestic targets. The threat that was coming was not from sleeper cells. It was foreign—but from foreigners who had infiltrated into the United States.[47]

The president's style of governance and level of engagement with the material can itself be interpreted as being a contributory factor in the 9/11 failure. No NSC meetings were called to discuss the threat outlined in the August 6th briefing, and the Commission could find "no indication of any further discussion before September 11 among the President and his top advisers of the possibility of a threat of an al Qaeda attack in the United States." One reason for this is that the president retired to his Texas ranch for the summer. Director of Central Intelligence (DCI) Tenet visited him there on August 17th but "did not recall any discussions with the President of the domestic threat during this period."[48] The report saw "little evidence that the progress of the plot was disturbed by government action. The US government was unable to capitalize on mistakes made by Al Qaeda. Time ran out."[49] Clearly this raises the question of political failure.

THE "POLITICAL" FAILURE

Intelligence is inevitably about conveying uncertainties and probabilities. But even if collection is as good as possible and analysis gets it right, the professionals may fail if their product does not convince policy makers of the need to act accordingly. Just as there are various causes of intelligence failure, so there are varieties of political failure: executives may fail to maintain an environment within which critical analysis can be conducted, they may dictate or manipulate the production of particular kinds of intelligence, or they may just select that which supports their predispositions while ignoring or rejecting anything that does not.

Richard Betts has argued:

> In the best-known cases of intelligence failure, the most crucial mistakes have seldom been made by collectors of raw information, occasionally by professionals who produce finished analyses, but most often by the decision makers who consume the

> products of intelligence services. Policy premises constrict perception, and administrative workloads constrain reflection. Intelligence failure is political and psychological more often than organizational.[50]

Similarly, for Christopher Andrew, "The historical record suggests . . . that the points at which the intelligence cycle most frequently breaks down are in the assessment process and the policy interface rather than in collection."[51]

There is an inevitable tension here: in democratic societies it is elected politicians, not salaried officials, who make policy decisions. Inevitably, policy makers have their own preferences based on their own backgrounds, experiences, interests, and worldview, and they (like the rest of us) have a tendency to resist information that conflicts with those. Therefore, analysts face an uphill task: "Intelligence is part of the government system, and has to have empathy and credibility with the policy-makers it serves. It cannot adopt an Olympian objectivity, or detach itself completely from government's policies and preconceptions. It has to sell its product, and has to be sensitive to its audience to do so."[52] But, in selling their product, the very problem for analysts is that it rarely meets the level of certainty that politicians, as men and women of action, demand. But if analysts struggle to "sell" their work to the policy makers, the latter may also struggle to sell their policies to the public.

The main body of the SSCI Report appears to absolve policy makers of responsibility for the intelligence failure, concluding that it found "no evidence that the IC's mischaracterization or exaggeration" on Iraqi WMD was "the result of political pressure."[53] Further still, it blames the intelligence community for not "accurately or adequately" explaining to policy makers the uncertainties that lay behind the catalogue of erroneous judgments contained in the NIE.[54]

However, it is not at all clear that *groupthink* identified by the SSCI as operating in this case—"examining few alternatives, selective gathering of information, pressure to conform within the group or withhold criticism, and collective rationalization"[55]—were not themselves consequences of individual perceptions of political pressure. The regular visits to CIA headquarters by Vice President Dick Cheney, a key advocate of the case for war between September 2001 and February 2003, were not held to have influenced the thrust of analysis on Iraq.[56] Nor is it clear that the managerial failure to utilize mechanisms designed to test analyses was attributable solely to a shared set of presumptions rather than, at least in part, to their close proximity to policy makers who had been making the case for a developing and threatening Iraqi WMD program for months prior to the drafting of the October 2002 NIE. In this respect, "managerial failure" could be interpreted as a euphemism for "politicization." Moreover, the SSCI had to reconcile the fact that, anonymously, a number of officials had been prepared to voice concerns but were unwilling to be publicly identified.[57] Ironically, it is not at all clear that, in this area of inquiry, the SSCI itself adopted the best analytical practices it identified as being absent from the intelligence effort on Iraq.

Silberman-Robb was not authorized to investigate how policy makers used the intelligence they received, but it still dismissed charges of politicization and, like the SSCI, criticized the intelligence community for failing to communicate effectively with policy makers.[58] Nevertheless, in dismissing charges of politicization, it did come far closer than the SSCI to recognizing the pressures emanating from the White House, to the extent that its conclusion on politicization can be regarded as somewhat contradictory:

> We closely examined the possibility that intelligence analysts were pressured by policymakers to change their judgments about Iraq's nuclear, biological, and chemical weapons programs. The analysts who worked Iraqi weapons issues universally agreed that in no instance did political pressure cause them to skew or alter any of their analytical judgments. That said, it is hard to deny the conclusion that intelligence analysts worked in an environment that did not encourage scepticism about the conventional wisdom.[59]

The detailed investigations into Iraq have shown clearly that there *were* failures within intelligence processes—in terms of collection, analysis, and dissemination. However, the official diagnosis of the problem, as represented in the official inquiries referred to here, is incomplete. This conclusion results from a combination of the following factors: the obvious desire of U.K./U.S. governments to present the case for war as though the intelligence left them no option but to disarm Iraq forcibly and the failure of official oversight bodies to identify clearly the extent to which intelligence (processes and products) were misused in order to mislead the public. All governments are prone to present their chosen course of action in definite terms; having made decisions, they are reluctant to invite further public debate and criticism. But, in this case, the stakes were much higher, involving military invasion, and there is a growing body of evidence that this gulf reflected not just politicians' customary "oversimplification and exaggeration"[60] and shows that the intelligence could never sustain the policy upon which the governments had determined at least a year before the invasion.

Space does not allow a detailed dissection of this, but the job has already been done by John Prados with respect to the United States.[61] He takes a series of key documents—for example, the CIA White Paper on Iraq's WMD of October 2002, President Bush's Cincinnati speech of October 2002, his State of the Union address of January 28, 2003, and Secretary of State Powell's remarks to the UN Security Council of February 5, 2003—subjects them to detailed scrutiny in terms of the then available intelligence, and demonstrates the growing gulf between them.

Thanks to the Butler Review in the United Kingdom we can make a similar comparison.[62] In March 2002—one year before the invasion—the Joint Intelligence Committee (JIC) provided an assessment that "intelligence on Iraq's WMD and ballistic missile programmes is sporadic and patchy." On nuclear weapons, "there is very little intelligence." Similarly, "there is very little intelligence

relating to [Iraq's chemical warfare programme]."[63] Six months later the JIC said: "Intelligence remains limited and Saddam's own unpredictability complicates judgements about Iraqi use of these weapons. Much of this paper is necessarily based on judgement and assessment."[64]

Thus, the intelligence failure regarding Iraqi WMD was partly a collection failure and partly an analytical failure—a failure to interpret correctly the meaning of the absence of information regarding WMD. Instead of interpreting the absence as evidence of destruction, it was interpreted as evidence of continued deception by the regime—an understandable error given the history of the regime and of the temptation for analysts to play it safe, but it was a failure all the same.

But, in Blair's foreword to the September 2002 dossier we read: "What I believe the assessed intelligence has established *beyond doubt* is that Saddam has continued to produce chemical and biological weapons. . . . I am in no doubt that the threat is serious and current."[65] And, in the Commons on September 24, 2002, Blair said: "The intelligence picture . . . is *extensive, detailed and authoritative*."[66] This was clearly highly misleading.

Thus the far greater failure was political. As we know now, in March 2002 Blair's foreign policy adviser, David Manning, met with Condoleezza Rice and assured her that Blair would not budge in his support for regime change.[67] In April 2002 Blair told Bush that the United Kingdom would support military action to achieve regime change in Iraq and from summer onwards bombing of Iraq was increased steadily in order to try to provoke Saddam Hussein into some response that would provide a pretext for war.[68] In July 2002 C (head of SIS) reported back to Downing Street on his recent Washington talks:[69] "There was a perceptible shift in attitude. Military action was now seen as inevitable. Bush wanted to remove Saddam, through military action, justified by the conjunction of terrorism and WMD. But the intelligence and the facts were being fixed around the policy."[70] But the only possible legal justification for invasion was Iraq's failure to disarm in line with UN resolutions passed after first Gulf War. Since Blair knew that he could not carry his party with him without such legal justification, the crucial role for intelligence was to support or rationalize the case regarding WMD.

So, power (the policy decision to invade Iraq) clearly led to explicit or implicit pressures within agencies during 2002 that saw judgments "firmed up" unjustifiably. But what was selected for public presentation and how it was presented by political leaders amounted to a clear deception.

CONCLUSION

The case of 9/11 illustrates elements of both intelligence and political failure, though it is difficult with this kind of surprise attack to imagine how intelligence might have been structured to prevent it. As an analytical device, we can ask the "what if" question. For example, even if President Bush had reacted to

the August PDB and all the disparate pieces of information that we now know about had been connected, the intelligence would still have amounted only to a general warning of possible hijacks within the United States at some unspecified future time. Assuming that the airline security and law enforcement communities then responded to this warning, their procedures would not have been sufficiently robust to prevent the seizure of all four planes on September 11. In the case of Iraq, what if the actual uncertainties regarding the presence of WMD in Iraq had been accurately and regularly communicated to the decision makers—would they have not invaded Iraq? Here, the evidence suggests strongly that it would have made no difference, because the U.S. and U.K. governments were determined on regime change by spring 2002 despite the weak intelligence then existent. Thereafter, the contribution of intelligence to the policy was as a tool to be utilized in selling that policy to skeptical publics, other countries, and ultimately the UN, and this was the context within which it was steadily firmed up. Therefore, although Iraq may also represent a messy mixture of intelligence and political failure, the latter was more serious and primarily responsible for the subsequent costly debacle in Iraq.

As a result of these commissions and inquiries there has been a great debate, primarily in the United States, as to how intelligence might be reformed in order to prevent a recurrence of failures. Even if one acknowledges that changes must include policy and practices, not just structures,[71] we must note that the potential for reform is seriously limited. The combination of cognitive and organizational pitfalls endemic within information and intelligence processes should alert us to the probability that reforms will have no effect.[72] Betts argues:

> Observers who see notorious intelligence failures as egregious often infer that disasters can be avoided by perfecting norms and procedures for analysis and argumentation. This belief is illusory. Intelligence can be improved marginally, but not radically, by altering the analytic system. The illusion is also dangerous if it abets overconfidence that systemic reforms will increase the predictability of threats.[73]

Of course, no extent of organizational reforms within intelligence can have the slightest impact on the possibility of political failures.

Finally, these events and subsequent inquiries indicate an enormous need for public education[74] and vigorous oversight. Given the long history of secrecy within which security intelligence has operated, it is not surprising that the public misunderstands its role. Now that intelligence is (partly) out of the box, it will not be possible to get it back in. Therefore, the task of explaining the potential and limits of intelligence is an urgent one for governments, practitioners, oversight committees, and scholars. It is a fundamental expectation of governments that they will provide public security and, in their urge to reassure the public, even well-intentioned politicians may be tempted to exaggerate the possibility that they can provide it. If, as in the case of Iraq, governments exaggerate threats and misuse intelligence in order to bolster their claims, they are culpable of serious dereliction

of duty. Since 9/11 there has been some soft-pedalling on oversight because of the false perception that this will somehow hinder greater intelligence efficiency; the Iraq debacle has reinforced the need for energetic oversight to reduce, though it cannot eliminate, the likelihood of future intelligence and political failures.[75]

NOTES

1. Respectively, T. H. Kean and L. H. Hamilton, *The 9/11 Report: The National Commission on Terrorist Attacks Upon the United States* (2004), available at http://www.9-11commission.gov/report/index.htm; L. H. Silberman and C. S. Robb, *Report* (Washington, DC: Government Printing Office for the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005), available at http://www.wmd.gov/report/report.html.

2. The most significant one that is discussed here is Butler, *Review of Intelligence on Weapons of Mass Destruction*, HC898 (2004), available at http://www.butlerreview.org.uk/report/.

3. M. Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996), p. 228.

4. Kean and Hamilton, op cit, pp. 339–48.

5. Ibid., p. 355.

6. R. Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962), p. 392; cf. also J. Sheptycki, "Organizational Pathologies in Police Intelligence Systems," *European Journal of Criminology* 1 (2004), pp. 315–16.

7. Kent Center for Analytic Tradecraft, *Making Sense of Transnational Threats*, Sherman Kent School, Occasional Papers (3:1, October, 2004), p. 4.

8. M. M. Lowenthal, *Intelligence: From Secrets to Policy*, 2d ed. (Washington, DC: CQ Press, 2003), pp. 92–93.

9. R. Mandel, "Distortions in the Intelligence Decision-Making Process," in S. J. Cimbala, *Intelligence and Intelligence Policy in a Democratic Society* (Ardsley-on-Hudson, NY: Transnational Publishers, 1987), pp. 69–83.

10. L. K. Johnson, *America's Secret Power: The CIA in a Democratic Society* (New York: Oxford University Press, 1989), pp. 76–99; Sheptycki, op. cit.

11. Mandel, op. cit., p. 73.

12. Kean and Hamilton, op. cit., p. 77.

13. The following section draws on chapter 7 of P. Gill and M. Phythian, *Intelligence in an Insecure World* (Cambridge: Polity, 2006).

14. SSCI, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq* (Washington, DC: Government Printing Office, 2004), available at http://intelligence.senate.gov/iraqreport2.pdf 1.

15. Ibid., p. 14.

16. Ibid., p. 15.

17. Ibid., p. 25.

18. Butler, op. cit., paras 402–5.

19. SSCI, op. cit., p. 14.

20. Ibid., p. 75.

21. Ibid., pp. 77, 80–81.

22. Butler, op. cit., paras 490–503.
23. SSCI, op. cit., p. 18.
24. Butler, op. cit., para 458.
25. SSCI, op. cit., pp. 23–24.
26. Ibid., p. 26.
27. Ibid., pp. 27–28.
28. Ibid., pp. 128–29.
29. Butler, op. cit., paras 566–78.
30. Silberman and Robb, op. cit., p. 10.
31. BBC, "A Failure of Intelligence," *Panorama*, BBC1, broadcast 11 July, 2004.
32. B. Woodward, *Plan of Attack* (New York: Simon & Schuster, 2004), p. 197.
33. Kean and Hamilton, op. cit., pp. 353–60.
34. Ibid., p. 417.
35. For example, see ibid., p. 143; also Lowenthal, op. cit., pp. 100–1.
36. SSCI, op. cit., p. 17.
37. Butler, op. cit., para. 45.
38. Ibid., para. 603.
39. Ibid., para. 45, fn. 13.
40. Ibid, para 604.
41. Foreign and Commonwealth Secretary, *Review of Intelligence on Weapons of Mass Destruction: Implementation of Its Conclusions*, Cm6492 (London: Her Majesty's Stationary Office, 2005), paras. 29–30.
42. Herman, 1996, op. cit., p. 235; A. N. Shulsky and G. J. Schmitt, *Silent Warfare,* 3d ed., (Washington, DC: Brassey's, 2004), p. 59.
43. Kean and Hamilton, op. cit., pp. 344–48.
44. R. A. Clarke, *Against All Enemies: Inside America's War on Terror* (London: Simon & Schuster, 2004).
45. Kean and Hamilton, op. cit., p. 366.
46. Ibid., pp. 261–62.
47. Ibid., p. 263.
48. Ibid., p. 262.
49. Ibid., p. 277.
50. R. K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31 (1978), p. 61.
51. C. Andrew, "Intelligence, International Relations and 'Under-theorisation,' " *Intelligence and National Security* 19 (2004), p. 172.
52. M. Herman, "Threat Assessments and the Legitimation of Policy?" *Intelligence and National Security* 18 (2003), p. 177.
53. SSCI, op. cit., p. 16.
54. Ibid.
55. Ibid., p. 18.
56. Ibid., pp. 275–76, 285.
57. Ibid, p. 272.
58. Silberman and Robb, op. cit., p. 5.
59. Ibid., p. 11.
60. R. Aldrich, "Whitehall and the Iraq War: The U.K.'s Four Intelligence Enquiries," *Irish Studies in International Affairs* 16 (2005), p. 74.

61. J. Prados, *Hoodwinked: The Documents That Reveal How Bush Sold Us a War* (New York: New Press, 2004).

62. A fuller analysis is provided in P. Gill, "Keeping in Touch With 'Earthly Awkwardness': Failures of Intelligence Analysis and Policy in the U.K.," in *Reforming Intelligence Across the World: Institutions and Cultures,* ed. T. Bruneau, (Austin: University of Texas Press, forthcoming).

63. Butler, op. cit., paras. 270–75.

64. Ibid., para. 295.

65. Her Majesty's Government, *Iraq's Weapons of Mass Destruction: The Assessment of the British Government*, September 24, 2002, available at http://www.the-hutton-inquiry.org.uk/ (emphasis added).

66. Butler, op. cit., para. 464. Emphasis added by Butler.

67. D. Manning, "Your Trip to the U.S.," Memo to the Prime Minister, March 14, 2002, available at http://slate.msn.com/id/2120886/June 20 2005.

68. M. Danner, "The Secret Way to War," *New York Review of Books*, June 9, 2005, pp. 70–74; M. Smith, "Blair Hit by New Leak of Secret War Plan," *Sunday Times*, May 1, 2005.

69. This is described in J. Risen, *State of War: The Secret History of the CIA and the Bush Administration* (London: Free Press, 2006), pp. 113–15.

70. M. Rycroft, "Iraq: Prime Minister's Meeting, 23 July 2002," available at http://slate.msn.com/id/2120886/ June 20 2005.

71. J. E. Sims and B. Gerber, "Introduction," in *Transforming U.S. Intelligence,* eds. J. E. Sims and B. Gerber (Washington DC: Georgetown University Press, 2006).

72. For example, Herman, 1996, op. cit., p. 230.

73. Betts, op. cit., p. 61.

74. cf M. Turner, *Why Secret Intelligence Fails* (Dulles, VA: Potomac Books, 2005), pp. 145–47.

75. These arguments are developed in more detail in Gill and Phythian, op. cit.

10

INTELLIGENCE OF THE PAST; INTELLIGENCE FOR THE FUTURE

HAROLD M. GREENBERG

ON FEBRUARY 22, 1946, U.S. DIPLOMAT George F. Kennan cabled Washington and laid the strategic groundwork of American foreign policy for the next four decades. The resulting "long telegram" pronounced the origins, characteristics, and probable course of Soviet behavior. Kennan's ideas addressed both immediate questions about Stalin's outward antagonism and spawned permutations of "containment" through the Reagan administration.[1]

Historians remember Kennan's cable as one of the Cold War's defining documents. Less often, however, is it recognized as the most important—and perhaps the most instructive—piece of finished strategic intelligence in American history. Admittedly, it is imperfect in this regard: At 8,000 words, the text is a shade too long to serve as a model for emulation; its recommendations violate the sacred gulf between intelligence analysis and policy making; and a wide circulation—which included Stalin himself—compromised the secrecy of Kennan's insight.[2]

In the history of U.S. strategic intelligence, the episode is nonetheless remarkable. In February 1946 the U.S. government had nothing akin to the mammoth intelligence community of the later Cold War. The Central Intelligence Agency (CIA) would not be established for nearly a year and a half—the National Security Agency (NSA) for six years—and the state of American foreign intelligence analysis lacked time-tested experience if not a theoretical framework. Kennan, a State Department foreign service officer stationed in Moscow, was no intelligence specialist. He relied on no sophisticated network of case officers or spies and no vast library of meticulously catalogued reference materials. Despite these apparent deficiencies, Kennan's intelligence was invaluable. It was critical and objective, and it served the precise needs of American policy makers at the time.

So how did Kennan do it? The answer paints a rather mundane picture of strategic intelligence even compared to the craft as it was practiced during the Cold War: Kennan had no need for gadgetry, purloined documents, or back-alley rendezvous. In short, he harnessed only his intellectual gifts and the skills of his academic training to draw profound meaning from first-hand observations of the Soviet regime.

SHERMAN KENT'S SHADOW

America's war of the 21st century seems to require novel policy approaches, especially in the field of intelligence. But Kennan's profound efficacy suggests that revisiting the wisdom of the past may be a more constructive first step. Recent intelligence woes—including the failures to learn of the 9/11 attacks and to accurately assess Iraq's weapons of mass destruction (WMD) programs—showed that a vast bureaucracy fed by a gargantuan budget cannot alone provide reliable analysis. Recent controversy surrounding NSA surveillance of American citizens suggests that our means of collecting intelligence are sorely mismatched with our means of ensuring its usefulness.[3] More money, more technology, and more reorganization do not address these underlying problems. To find the answers, it is worth revisiting the fundamental tenets that guided our intelligence community at its birth.

Sherman Kent's classic 1949 book, *Strategic Intelligence for American World Policy*, is a good starting point.[4] A Kennan contemporary, Kent may rightly be called the founding father of American intelligence analysis. Like many of his fellow Yale graduates, he joined the Office of Strategic Services (OSS), America's wartime intelligence and covert action unit, after the United States entered World War II.[5] There he gained experience not on the front lines, but as chief of the Europe-Africa division of the Research and Analysis Branch. He returned to the United States at war's end to teach alongside Kennan at the National War College. Brief stints at the State Department Office of Research and Intelligence and the Yale University Department of History as well as the publication of *Strategic Intelligence* anticipated his permanent return to government service in 1950 at the new CIA. He spent the next seventeen years at the Agency, most of it as Assistant Director for National Estimates. His contribution to the theory and practice of intelligence analysis has been prodigious. He was instrumental in the creation of *Studies in Intelligence*, the CIA's in-house intelligence journal, and the CIA's analytical training academy now bears his name.[6]

By 1949, Kent could draw upon his wartime intelligence experience. But he could not yet reflect upon the standing intelligence bureaucracy of his future career. The ideas expounded in *Strategic Intelligence* are thus largely theoretical. Kent tells us what an ideal intelligence operation *would* look like; how it *should* function; what duties it *ought* to focus on in times of both peace and war. The 200-page book is a treatise, an opinion-laden guide rather than an effort to reform or

criticize. The timelessness of Kent's work leaves this task to us. Though the book is somewhat dated—the title itself recalls a different vocabulary for talking about U.S. national security—a review of Kent's design reminds us that the quality of our intelligence agencies is not solely a function of their structure. More alarmingly, it reveals that American society today is not particularly in touch with the needs of its intelligence community.

"INTELLIGENCE IS ORGANIZATION"

A look at Kent's work is appropriate in part because the United States is today fighting the battles of its past. The events of both fifty-five years ago and five years ago prompted major reorganizations of U.S. national security institutions and the creation of new ones. In each case, statutory changes shuffled the federal bureaucracy: The National Security Act of 1947 consolidated the armed services into the expansive Department of Defense; the more recent Homeland Security Act of 2002 dumped twenty-two scattered agencies into a new Department of Homeland Security.[7] In each case, plans for reform kept intelligence agencies separate from the policy makers they served. The 1947 Act created the CIA as an independent executive agency. The Intelligence Reform and Terrorism Prevention Act of 2004 implicitly reaffirmed the wisdom of the CIA's independence and established the Office of the Director of National Intelligence (DNI) to coordinate intelligence across the U.S. government.[8]

If Congress had left it up to Kent, our intelligence establishment would look and work far differently. His vision called for a scattered community of intelligence bureaus housed within the departments of the executive branch. It would be decentralized and subject to a small and lean central oversight agency with investigatory powers. The bureaus themselves would be specialized according to the "jurisdictional competence" of their parent departments. Today, Kent's archaic language conveys the obvious advantages of a division of labor. Who better than the U.S. Air Force, he asks, can evaluate intelligence on foreign military aviation?[9]

For Kent, the greatest virtue of sprawling intelligence responsibilities throughout the government is its uniting intelligence producers with policy makers. He deals with this subject of "utmost delicacy" and importance in his chapters on intelligence methods. But this tenet is the cornerstone of his organizational philosophy; it is insufficient, but wholly necessary, for the success of the intelligence cycle.[10] Kent writes:

> Even within a single department, it is hard enough to develop the kinds of confidence between producers and consumers that alone make possible the completeness, timeliness, and applicability of the product. There are great barriers to this confidence even when intelligence is in the same uniform or building or line of work. But how much more difficult to establish confidence across the no man's land that presently lies between departments.[11]

Too great a distance between intelligence agencies and the consumers they serve would leave intelligence producers lost. "It would not be impossible," he continues, "for such an organization to misdirect its efforts, watch the wrong developments, and report on matters of small concern."[12] The critical proximity, Kent suggests, alleviates the problem of policy makers' lack of engagement rather than the aloofness of a central intelligence agency.

The importance of a close relationship is indisputable. R. James Woolsey, Director of Central Intelligence from 1993 to 1995, resigned from office rather than serve without regular access to President Clinton.[13] But recent events have focused criticism on the excessive intimacy of intelligence consumers and producers rather than their disconnectedness. Kent, arguing against a dominant, central intelligence organization, writes, "there would be little disposition to revere the opinions and facts produced by the agency just because it was *central*."[14] The Bush administration's close liaison with the CIA over Iraqi WMD programs and Saddam Hussein's relationship to Al Qaeda suggests that centralized intelligence does not necessarily preclude the kind of interaction Kent views as essential. The bigger question is the character of policy makers' close relations with intelligence agencies because interaction is not by definition benevolent. Paul R. Pillar, the senior U.S. intelligence officer for the Near East and South Asia between 2000 and 2005, has alleged that the Bush administration corrupted the intelligence cycle with selective and politicized use of CIA estimates to justify war. The intelligence community, he writes, "was pulled over the line into policy advocacy."[15]

Years from now, historians will make judgments about the veracity and extent of these claims. Today, the controversy gives us further reason to heed Kent's caveats about the relationship between policy makers and central intelligence. Perhaps Kent was wrong to think that a nondepartmental organization would inspire little consumer confidence in its analysis. But it is possible that a central agency responsible for the lion's share of foreign, strategic intelligence may be more subject to manipulation of its analytical product—unwitting or not—than a federated intelligence community. Kent's worries about central intelligence persist, but for reasons few appreciated until recently.

Few in the political mainstream today would agree that dismantling the CIA and distributing its responsibilities among the Cabinet departments is wise or practical. It likely would create problems as serious as those it solved: Some intelligence topics—notably terrorism—do not fit into neat categories paralleled in the structure of the federal government. Would the department or departments assigned responsibility for the hot-button security issues become the "favorites" of intelligence consumers; how would departments with little interest or experience in intelligence react to new demands; last, what bureaucratic problems would result from the dual reporting of such agencies to both department and White House policy makers? Upheaval over the organization of the Federal Emergency Management Agency (FEMA) highlights the difficulty of requiring agencies accountable ultimately to the president to report through an additional

layer of departmental bureaucracy.[16] The uncertain role of the DNI would further complicate this effort.

In spite of these questions, departmental intelligence may have a place alongside central intelligence. In a 1950 review of Kent's then-new book, University of Chicago geographer Norton S. Ginsburg wrote, "Intelligence derives its *raison d'etre* from conflict, whether in times of peace or war. Its goal at all times is not the maintance [sic] of peace nor the provocation of war, but preparedness for the latter." The creation of America's intelligence bureaucracy in the early Cold War indeed reflected U.S. susceptibility to surprise attack and the increasingly destructive potential of armed conflict in the nuclear age. But it does not exist today solely for that reason. Though Kent's departmental model did not prevail in his own time, it may be uniquely suited for our age, in which "actors" no longer constitute the totality of menaces and wars are no longer restricted to battlefields.[17]

The looming threat of avian influenza is a good example.[18] Tracking the spread of dangerous pathogens may not prevent their reaching American shores, but it may provide enough advance warning to mitigate economic damage and loss of life. The Department of Health and Human Services (HHS) may be best equipped to track the nascent outbreak of disease and evaluate the danger to the United States. A biomedical intelligence unit could employ scientists and epidemiologists to report on the progress of dangerous pathogens and new technological means of engineering harmful biological agents. HHS intelligence might also include professional intelligence officers who can judge the activities and movements of foreign scientists and gauge what expertise they might bring to terrorist organizations and belligerent states. HHS may also serve as a link between the intelligence community, which collects such information overseas, and the Department of Homeland Security, which must help local and state governments implement policies to cope with public health crises. Assigning bio-intelligence to the lead department for preventing and containing the outbreak of disease also moderates the consequences of information hoarding. The 9/11 Commission criticized "the culture of U.S. intelligence agencies feeling they own the information they gathered at taxpayer expense."[19] Perhaps organization alone cannot correct the reluctance of intelligence agencies to share information, but reducing the need to disseminate information beyond a single federal department may stem lapses due to territorialism.

To be sure, structural changes are no panacea for the flaws of a bureaucracy. The beauty of Kent's organizational ideas is not that they provide a template for U.S. intelligence to cope with a radically different security environment. Rather, Kent designed an intelligence community that would be best suited to handle the challenges of a complex and uncertain world. Consider Kent's eerily perspicacious argument in favor of foreign surveillance: "In the world of international relations," he writes, "these parties in the conspiracy may be residents of half a dozen countries, and the story what they are up to, if ever pieced together, must be pieced together from fragments supplied from the half-dozen different national

sources." By Kent's own admission, an element of paranoia characterizes this outlook; threats may come from anywhere, and despite his strong reservations about central intelligence, he recommends a "clearing house in a central spot" to piece together nebulous plots against American interests.[20] At a time when the nexus of American fears was the Kremlin, Kent resisted the temptation to focus the work of U.S. intelligence on Moscow, the Soviet Union, and though he probably did not realize it, nation-states in general. A list of specific priorities for intelligence collection and analysis, Kent believed, "would have neither the cheering element of certainty nor the comforting quality of logic."[21] Concentrating on the broad themes of human activity, such as political, economic, and technological change, on the other hand, rendered intelligence analysis adaptable to specific, acute dangers. Adaptability provided greater assurance that schemes of all origins—even those unknown—could be detected. Kent never advocated observing the entirety of world events. Rather, his aim was to avoid starting too narrowly. The moral is not simply to organize intelligence with a broad range of threats in mind or to exhort greater information sharing among government agencies; it is also to recruit and train minds able to discriminate, reason about, and divine the meaning of abstract change. This challenge is more staggering than any problem of bureaucratic organization.

"WELL-STOCKED BRAIN CELLS"

Kent was first and foremost an historian. A career as a junior professor at his alma mater predated his life as intelligence professional and theorist. As a teacher, he was known for his acerbic wit and strict insistence on analytical rigor, qualities that infuse his book.[22] Kent brought an academic sagacity to the work and study of intelligence, and it is not surprising that he was a theorist as well as a practitioner of historical analysis. The overarching principles of sound analytical methodology, he believed, applied to all realms of rational inquiry. Harold P. Ford, a CIA Office of National Estimates veteran, aptly observed that in Kent's first book, *Writing History*, which he completed at Yale, one "need only substitute the words 'intelligence officer' for 'historian' " to appreciate Kent's faith in the transferability of a critical disposition.[23]

Kent gave up a promising academic career to become a professional intelligence analyst. Many of his Ivy League peers also eagerly joined CIA ranks in the Agency's early years. Nonetheless, the quality of CIA employees in Kent's time was by no means unquestionable, and Kent takes time in *Strategic Intelligence* to reflect on personnel problems in both the CIA and government in general.[24] Principal among Kent's concerns were the "two forces of disintegration" that, in his time, lured intelligence agencies' most competent and valuable employees away from government service. The first was the result of postwar budget cuts and the reinstitution of civil service regulations, which dismissed personnel without regard to talent or ability. The second was the attraction of

intelligence professionals to the private sector, which in Kent's view precipitated the catastrophic decimation of the intelligence community after the war.

The latter problem persists to this day. Washington, DC, area newspapers routinely advertise private-sector job fairs for civil servants with active security clearances. In a recent article on attrition in the CIA clandestine service, *U.S. News & World Report* reported that government contractors such as Blackwater USA, Science Applications International Corp., and Abraxas are luring mid-career CIA officers with offers of $200,000 per year or more, sums far in excess of even the highest civil-service salary grades.[25] The attraction of private-sector opportunities to fresh university graduates compliments the exodus of experienced intelligence analysts and clandestine officers. The overwhelming cost of a university degree, the lucrative prospects of a career in business consulting or investment banking, and the time required to obtain a security clearance all seem to have diluted the rewards of government service for America's brightest and best educated. Even students unwilling to abandon the prospect of government work find that they command a higher salary as a contract employee than on the government payroll.

The recruitment problem is not merely a question of luring young, educated professionals away from enticing opportunities elsewhere. One hundred twenty thousand people applied to the CIA in 2005. But "not just anyone," Kent tells us, "can hold a professional job in an intelligence organization." The strength of raw numbers fails to address the great need for personnel with "the best in professional training, the highest intellectual integrity, and a very large amount of worldly wisdom."[26] According to Kent, superior intelligence analysts are imaginative thinkers, and they must have an acute understanding of the problems of U.S. foreign policy. They may have specialized area knowledge or language skills, but unassailable abstract reasoning skills are paramount. The academic analog is obvious. An intelligence organization, Kent writes, must resemble a "large university faculty," albeit one working at the pace and with the deadlines of a daily newspaper.[27]

Kent undoubtedly saw the academy as an ideal training ground for budding intelligence analysts. Today, the need for personnel with first-rate intellectual credentials is as urgent as it was in Kent's time. But the radically different character of undergraduate education in America has imposed staggering new challenges to the cultivation of a strong analytical corps. Two trends in particular have detached the preparation of the university from the needs of strategic intelligence. The first is the narrowing of the liberal arts curriculum. Undergraduates today pursue specialized courses of study that decades ago were the exclusive province of graduate students. At Yale, Kent's alma mater, undergraduate history majors must take courses from a variety of geographic and epochal divisions. Though some introductory courses survey broad periods and topics, the vast majority of department offerings reflect the very specific research interests of the faculty, which often favors episodic snapshots of already narrow historical subcategories. This may be an exceptional means of learning the discipline of history,

but it leaves graduates with little experience reasoning about the wide-ranging themes that Kent tells us is integral to intelligence analysis.

Students themselves have also changed the character of college education. The pressure to complete a major course of study notwithstanding, many undergraduates, absent a list of compulsory courses, are loath to venture beyond their intellectual comfort zones and avoid courses and disciplines outside their areas of interest or ability. This academic risk aversion reflects the growing career orientation of the liberal arts as well as many students' careful stewardship of their grade point averages in preparation for the job market. Remaining competitive for top jobs today demands substantial course preparation specific to the industry or field in question. Among students, this tendency is by no means pervasive, but it is far more prevalent now than in Kent's time. The result is throngs of intelligent, young college graduates whose knowledge and experience lies within an extremely limited subject area. This is no tragedy for most of their future employers. But for the government's intelligence agencies, it aggravates an already problematic recruiting environment. It is true that some areas of strategic intelligence require a kind of specialized expertise attainable only via higher education. But the mastery of a body of knowledge alone is insufficient for the demands of intelligence analysis. Kent again: "In this case, what I am speaking of is not the important but gross substance which can be called recorded fact; it is that subtle form of knowledge which comes from a set of well-stocked and well-ordered brain cells."[28]

The second trend is the elimination of courses most relevant to strategic intelligence. To continue with the example of Kent's field, most history departments in the United States offer a wide variety of lectures and seminars on topics spanning the entirety of historical study. But for the past several decades, broad surveys of political, diplomatic, and military history have become increasingly scarce. So have courses on U.S foreign policy. Social and cultural history, which examine society apart from political power, now comprise the bulk of course offerings in most history departments. This is not to say that this approach is insignificant to intelligence analysts. Indeed, a sophisticated understanding of the social and cultural movements of the Middle East and the Islamic world, for example, is more important than ever to the work of U.S. intelligence. The problem is that in many academic disciplines students are often exposed to these subfields at the expense of equally important others. Intelligence analysts weigh the outcomes of political developments and policy choices, but many college students today never study great political conflicts, strategic thinking, or the strategic thinkers that have shaped the present conduct of world politics. Intelligence analysts must provide timely, useful information to policy makers at the highest echelons of government, but few graduates have studied in the classroom the ways in which government officials make foreign policy. Decades ago, the Naval War College developed its legendary strategy and policy curriculum from courses at nonmilitary institutions like Yale; now, these institutions should borrow their courses back.[29]

To counterbalance the difficulty recruiting the best and brightest, intelligence agencies must establish a campus presence at top universities comparable to that of private industry. They must offer comparable incentives, and most important, they must vigorously court students who have not only technical expertise, but who have wide-ranging academic experience and intellectual breadth, and "to whom research and rigorous thought," to borrow Kent's words, "are the breath of life."[30] Exposing students on campus to the demands of intelligence work may not reverse their career-mindedness, but it may help correct the widespread perception that specialization and careful academic preening is the only path to a rewarding career.

Kent's comparing intelligence agencies to universities also highlights the problems common to both institutions today. Apart from their mutual purpose of unearthing truth and creating knowledge, universities and intelligence agencies share remarkably similar managerial challenges. The most obvious example is the recent unrest among both the Harvard University faculty and the staff of the CIA, which converged along complaints over leadership. Director of Central Intelligence (DCI) Porter Goss and Harvard President Lawrence Summers each tried to reform organizations with defining senses of history and pride in their reputation among peers, enormous resources both human and financial, and staff composed mostly of skilled professionals whose length of tenure far eclipsed his own. Summers, who was a professor of economics at Harvard and returned in 2001 as university president after ten years in government, attacked Harvard's status quo head-on. With notorious confrontation, he pointed to undergraduate dissatisfaction with Harvard's educational offerings and challenged faculty to teach broader courses more in touch with student needs.[31] Goss, who spent ten years in the CIA clandestine service and returned as DCI in 2005, over three decades after his retirement, provoked similar ire among CIA staff. Some resented his apparent delegation of Agency management to aides brought from Capitol Hill and his aloofness from the rank and file. His proposal to revise the Agency's four-directorate structure, unveiled in early 2006, may explain Goss's unpopularity among the clandestine service, which he had apparently stripped of erstwhile preeminence within the CIA.[32]

Though dissatisfaction in Cambridge and Langley focused largely on management style, Goss's and Summers's terms should have sparked debate over the benefit for which these institutions exist. Both Harvard and the CIA serve high-paying customers who expect, in the former case, an education or, in the latter, objective analysis of secrets gathered from abroad. With admittedly controversial means, Goss and Summers re-emphasized the uncontroversial notion that their respective institutions should recommit themselves to their fundamental objectives. This is not to say that CIA staff and the Harvard faculty were unwilling to endorse change or that they stood unwavering against reform. It merely underscored the ways in which the internal politics and bureaucratic inertia of the CIA and Harvard University made rededication to the work for which they were established a contentious idea. Over time, these large bureaucracies have evolved

competing interests within their walls. Both the intelligence community Kent envisioned and the academy in which he taught were small, focused, and dedicated to specific, well-defined missions. The relevance of these institutions today depends upon keeping their significantly larger staff, greater resources, and more expansive purview sufficiently responsive to the narrow needs of those they serve. Old and storied organizations are not unique in this respect. The swelling Office of the DNI, created to coordinate the government's sixteen scattered intelligence agencies, may be falling victim to the same pattern of growth, distraction, and stagnation.[33] As for Goss and Summers, their stories reflect the sheer difficulty of reforming bureaucratic monsters from above. Both resigned—and were likely forced out—without affecting meaningful change.

INTELLIGENCE FOR THE FUTURE

Kent argues convincingly for a formidable analytical component to American strategic intelligence. But he fails to critically consider the limits of finished analysis to policy making. From *Strategic Intelligence*, one gets the sense that with perfect organization and perfect information, a competent intelligence analyst can calculate and forecast precise developments in any realm of world affairs. But immutable faith in the predictability of human behavior is a fallacy, and the complexities of our world have proved intractable to even the most sophisticated of thinkers. Kent is not wrong to expect that good analysis closely mimics a scientific process of hypothesis, testing, and re-evaluation, and it is true that the acquisition of the best information possible is essential. But the "compulsive preoccupation with *prediction*, with the elimination of 'surprise' from foreign affairs," as former intelligence analyst Wilmoore Kendall wrote in a review of Kent's book shortly after its publication, is not only unrealistic but obscures the most appropriate function of intelligence analysis.[34] That, Kendall continues, is "contingent" rather than "absolute" prediction: gauging likely outcomes based on a range of possible developments, choices, and scenarios. Both policy makers and the public should understand that intelligence agencies cannot and will not discover every scheme or foil every nefarious plot. Cries of "intelligence failure" are sometimes justified, but often they only demoralize professionals asked to perform impossible analytical feats.

In the course of policy makers' day-to-day decision making, contingent predictions are more helpful than half-hearted, unambiguous guesses about the origins and nature of future threats. Kent's analytical philosophy is not inconsistent with this notion. George Kennan's long telegram reveals precisely why. It underscores the timeless significance of critical analysis and the value of a broad understanding of the world at large. Kent articulates no model for a perfect intelligence community. His provisions cannot simply be borrowed for our benefit today. Nonetheless, his ideas are transferable. They reflect a wisdom that might serve the present as it served the past.

NOTES

1. John L. Gaddis, *Strategies of Containment*: *A Critical Appraisal of American National Security Policy During the Cold War*, revised and expanded edition (New York: Oxford University Press, 2005).

2. John L. Gaddis, *The Cold War: A New History* (New York: Penguin Press, 2005), pp. 29–30.

3. See Michael Hirsh, "Wanted: Competent Big Brothers," *Newsweek* (web-exclusive commentary), February 8, 2006, available at http://www.msnbc.msn.com/id/11238800/site/newsweek/from/ET/.

4. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press, 1949).

5. Rhodri Jeffreys-Jones, *The CIA and American Democracy*, 3d ed. (New Haven, CT: Yale University Press, 1989), p. 20; Robin Winks, *Cloak and Gown: Scholars and the Secret War: 1949–1961* (New York: Morrow, 1987), p. 35; Bradley F. Smith, *Shadow Warriors: OSS and the Origins of the CIA* (New York: Basic Books, 1983).

6. Harold P. Ford, "A Tribute to Sherman Kent," *Studies in Intelligence* (Fall 1980), available at http://www.cia.gov/csi/books/shermankent/1tribute.html; Jack Davis, *Sherman Kent and the Profession of Intelligence Analysis*, The Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol. 1, No. 5, November 2002, available at http://www.cia.gov/cia/publications/Kent_Papers/vol1no5.htm.

7. National Security Act of 1947, 50 U.S.C., Title I, Section 102; Homeland Security Act of 2002, Pub. L. No. 107–296 (2002).

8. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458 (2004). For the political background of the recent intelligence reform, see Helen Fessenden, "The Limits of Intelligence Reform," *Foreign Affairs* (November/December 2005), pp. 106–20.

9. Kent, p. 104.

10. Ibid., pp. 81, 180; see also Loch Johnson, *America's Secret Power: The CIA in a Democratic Society* (New York: Oxford University Press, 1989), pp. 76–99.

11. Ibid., p. 81.

12. Ibid., p. 82.

13. See R. James Woolsey, "Unprepared: 'Why America Slept' Before Sept. 11," *Opinion Journal* (October 21, 2003), available at http://www.opinionjournal.com/la/?id=110004195.

14. Kent, pp. 82–83 (emphasis in original).

15. Paul R. Pillar, "Intelligence, Policy, and the War in Iraq," *Foreign Affairs* (March/April 2006), pp. 16–17, 20. See also Murray Waas, "Insulating Bush," *National Journal* (April 1, 2006), pp. 36–40.

16. See Chris Strohm, "Gambling on Reorganization," *GovExec.com*, March 20, 2006, available at http://www.govexec.com/dailyfed/0306/032006ol.htm

17. Norton S. Ginsburg, "Strategic Intelligence," *Annals of the Association of American Geographers* 40 (1950), pp. 89–91. See also John L. Gaddis, *Surprise, Security, and the American Experience* (Cambridge, MA: Harvard University Press, 2004).

18. Mike Ahlers, "Chertoff: Bird Flu Possible in U.S. Within Months," *CNN*, March 10, 2006. See also Loch K. Johnson, *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security* (New York: NYU Press, 2002).

19. *Final Report of the National Commission on Terrorist Attacks Upon the United States* (9/11 Commission Report) (New York: W.W. Norton, 2004), p. 417.

20. Kent, p. 154.

21. Ibid., p. 31.

22. Davis, op. cit.; Ford, op. cit.

23. Ibid.

24. Jeffreys-Jones, pp. 70–71.

25. Linda Robinson and Kevin Whitelaw, "Seeking Spies: Why the CIA Is Having Such a Hard Time Keeping Its Best," *U.S. News & World Report,* February 13, 2006, p. 39. For federal pay scales, see http://www.opm.gov/oca/.

26. Robinson and Whitelaw, p. 37; Kent, pp. 74, 65.

27. Ibid., pp. 69–77.

28. Ibid., p. 65.

29. See Gaddis, *Strategies of Containment*, p. xiv.

30. Kent, p. 74.

31. John Tierney, "The Faculty Club," *New York Times*, February 25, 2006.

32. Robinson and Whitelaw, pp. 36–37; Paul de la Garza and Anita Kumar, "Porter Goss Ends His Stormy Tenure as CIA Director," *St. Petersburg Times*, May 6, 2006; Marc Mazzetti, "Exit of Chief Viewed as Move to Recast C.I.A.," *New York Times*, May 7, 2006.

33. Greg Miller, "Intelligence Office Has Swollen, House Panel Says," *Los Angeles Times*, March 31, 2006.

34. Wilmoore Kendall, "The Function of Intelligence," *World Politics* 1 (1949), p. 549 (emphasis in original). For more on this point, see also Jeffreys-Jones, p. 54.

11

NATIONAL INTELLIGENCE IN THE AGE OF TRANSPARENCY

KRISTIN M. LORD

WE LIVE IN AN AGE OF UNPRECEDENTED global transparency. More information is available to more people than ever before in human history. Thanks to the Internet, images captured with inexpensive camcorders or even cell phones can be disseminated around the world instantly. Satellite television broadcasts news worldwide, making government-sponsored news programs nearly irrelevant in many countries. Nongovernmental organizations like Global Witness, Transparency International, and the Stockholm International Peace Research Institute (SIPRI) collect and publicize information about human rights abuses, corruption, and arms transfers—the most sensitive of subjects. Electoral democracies, which release vast amounts of information about their policies and decision making, now number 119.[1] International organizations like the United Nations publish information about conventional weapons stocks with the goal of reducing the incidence of war.

Transparency is transforming the world. And, in many ways, it is doing so for the better. Transparency can be a great force for peace. It can reduce misperceptions and uncertainty, build security and confidence, and help societies to know each other better. Because of this potential, conventional wisdom prescribes transparency to cure a host of global ills ranging from conflict to corruption, dictatorship to development.

Yet transparency holds perils as well as promise.[2] It can highlight differences rather than shared values. It can show aggression and hate rather than cooperation and friendship. It can show violations of, not adherence to, global rules and norms. In certain circumstances, it can exacerbate conflicts and make war more likely. Transparency is a double-edged sword.

This chapter explores the dark side of global transparency and its implications for international security and national intelligence. Its goal is to persuade the

reader to question conventional wisdom about transparency and see the trend toward greater transparency for the complex phenomenon it is. Because protecting national security is the most pressing problem of intelligence agencies, this chapter focuses on the relationship between global transparency, security, and conflict. However, it is worth noting that transparency affects domestic governance, international governance, and the role of transnational organizations. Those dynamics influence national security as well, but they are beyond the scope of this chapter.

THE NATURE OF GLOBAL TRANSPARENCY

Transparency is a condition of openness in which information about the priorities, intentions, capabilities, and behavior of powerful organizations is widely available to the global public.[3] Transparency is morally neutral and is not synonymous with truth. It may reveal actual or perceived facts, actual or perceived falsehoods, behavior, intentions, ideas, values, and opinions. It may reveal neutral, empirically verifiable information or propaganda specifically designed to advance a particular cause or view. Transparency increases due to major initiatives by governments to open up but also through the cumulative effects of individuals or small organizations that spread information. Most significantly, transparency describes the relative availability of information, not its content.

Five factors increase global transparency: the spread of democratic governments, the rise of the global media, the spread of nongovernmental organizations, the proliferation of international regimes requiring governments to disclose information, and the widespread availability of information and communications technologies. Of these five factors, the first four involve organizations whose actions lead to the dissemination of information across borders. The last is a tool used by individuals or groups of individuals to disseminate information.

The implications of global transparency vary depending on what transparency reveals, who benefits, and how people interpret the information they receive. It depends on where people look for information and what information they believe. To understand the effects of greater transparency, analysts must strip away value-laden assumptions about what transparency will reveal. We should not assume that transparency will reveal harmony rather than conflict and tolerance rather than hate. We should not assume that, once information flows freely, people will interpret new information in a particular way or hold particular values.

Global transparency amplifies trends whether they are negative or positive and, for this reason, encourages both virtuous and vicious circles. If a government is genuinely peaceful, for instance, greater transparency makes others aware of this fact and gives them confidence in that assessment. That knowledge can lead those governments to reciprocate, which makes the first government more secure and reinforces efforts to improve relations on both sides. Evidence that peaceful

gestures are productive strengthens politicians who support such steps and encourages them to make further peaceful gestures. Because transparency can encourage virtuous circles of cooperation, deliberate acts of transparency can be effective confidence- and security-building measures when countries or groups are actively trying to improve their relations. However, aggressive actions or words can fuel vicious circles of confrontation and conflict if transparency shows ill will, a failure to comply with international agreements, arms build-ups, aggressive rhetoric, or a willingness to use force. Such acts will be evident and create pressure to reciprocate, fueling a vicious circle of distrust that can lead to violence if unchecked.

With respect to ideas and values, transparency makes them more widely accessible and, in so doing, may encourage collective action by letting people see how widely a particular sentiment—whether dissatisfaction with an oppressive or unpopular government (e.g., in pre-1979 Iran or Lebanon in 2005) or hatred toward a particular ethnic group (e.g., in Rwanda)—is shared. Evidence that ideas and values are held widely legitimizes those ideas and values and encourages their further spread, regardless of their content.[4] Transparency is indiscriminate. When ideas—whether anti-Americanism or belligerent nationalism—gain legitimacy and spread, they allow people to justify behaviors in which they did not previously engage, such as the use of violence. Evident mass support for an idea can also silence dissenters even if there are no formal penalties for speaking up. People may not be brave enough to distance themselves from the majority, they may fear social penalties, or people may question whether they are right if so many others disagree.

How people interpret information is as important as what transparency reveals. The meaning people draw from information depends on pre-existing ideas and values that can change slowly even when new information calls those views into question. To cope with the volumes of information received each day, people tend to interpret new information in the context of existing views and values and discard contradictory data. As the weight of contradictory evidence grows, most people will adjust their views accordingly.

In order to draw meaning from information, people assess the credibility of the source as well as the identities and reputations of the people or groups involved.[5] People are more likely to interpret favorably information about groups they like or trust and discount positive or ambiguous information about groups they distrust. Information is viewed through the lens of pre-existing values. The meaning of information, and therefore how people ought to respond to it, depends heavily on existing views about what is right and wrong, what actions are threatening or benign, who is an enemy or a friend, or who is part of an in-group and who is not. For instance, a Gallup poll released in February 2002 indicated that 61 percent of nearly 10,000 Muslims in nine Islamic countries do not believe Arabs were responsible for the terrorist attacks against the United States on September 11th of the previous year.[6] Observers had a hard time fitting the new information with their previously held beliefs. When antiterrorist ads produced by

the U.S. government were shown recently to focus groups in Jordan, the majority of respondents were simply puzzled, protesting, "But bin Laden is a holy man."[7] Regardless, at some point, when the incongruity between the previously held beliefs becomes significant enough, people may change their opinions.[8]

The role of trust and identity affects not only how people interpret news about people or groups where there is clearly a social relationship, but also how they interpret "tangible" data. For instance, though interpreting information regarding military capabilities seems concrete, it is deceptively complicated. Transparency can let us see how many tanks a country owns. It cannot tell us definitively whether those tanks are a threat. That assessment depends on how we assess the intentions of the owner as well as the owner's identity. If the owner is considered a friend, people are less likely to interpret the tanks as a threat, but if the owner is an enemy, the purchase of even a single new tank may seem dangerous.

The importance of social relationships in interpreting information means that governments may change their interpretation of an enemy's behavior reluctantly, even when there is substantial information that a long-standing enemy's intentions have become conciliatory. In the language of political science, mistrust as well as uncertainty drives the security dilemma. To give an example, after the Soviet Union signed the 1987 Intermediate-Range Nuclear Forces Treaty (INF Treaty), withdrew forces from Afghanistan in 1988, announced conventional force reductions in Europe, and acquiesced to the 1989 revolutions in Eastern Europe, some American policy makers still questioned Soviet motives.[9] Six months before the Berlin Wall fell, Secretary of State James Baker praised the Soviets for releasing political prisoners and reforming emigration policies but said, "We must all, I think, face the fact that the Soviets continue to pose a significant military threat. . . . For all the talk of 'defensive defense,' Soviet military exercises still continue to show a marked inclination for taking the offensive. For the all the talk of openness, the Soviets have yet to publish a real defense budget."[10] It took the extremely costly signal of acquiescing to the 1989 revolutions in Eastern Europe to convince American leaders that the Soviet Union had changed truly and irreversibly. Predicting behavior based on identity carries risks, however, and can lead people to misinterpret actions. For instance, as Michael Barnett notes in his work on the Middle East, Iraq failed to predict that Saudi Arabia would side against it in the 1990 Gulf War because the Iraqi government focused on Saudi Arabia's identity as an Arab state and therefore expected Saudi Arabia to ally with its fellow Arab state. Instead, Saudi Arabia acted as a typical sovereign state and defended its national interests, which Iraq threatened.[11]

TRANSPARENCY, SECURITY, AND CONFLICT

Scholars and policy makers make three main arguments to explain how greater transparency could increase national security and reduce conflict. First, transparency may clarify the intentions of governments and reduce

misperceptions. Second, greater transparency may reduce uncertainty about the military capabilities of states and prevent leaders from overestimating threats. Third, greater transparency may help people to know each other better and humanize other groups, making it harder to use violence against them. The following sections consider each of these arguments in turn.

TRANSPARENCY OF INTENTIONS

The idea that uncertainty and misunderstanding are root causes of international conflict holds wide support among political scientists and even the general public, though they may not all articulate their views quite that way. Transparency, by providing better information about the intentions of other governments, promises to clear up uncertainty and misunderstandings that prevent better international relations and make international conflict less likely.[12]

Theoretically, transparency could help to defuse the so-called security dilemma in which even peace-loving governments that only wish to protect their own security threaten other states nonetheless. Feeling insecure, a government may arm itself and consequently make neighboring states feel less secure as well. Because other states cannot know what that state intends to do with those new arms, those states take steps to protect their security in response, creating a spiral of suspicion and insecurity despite the fact that none of the parties harbors aggressive intentions. This security dilemma—an unfortunate but rational response to an international system in which governments must ensure their own security—is blamed for international conflict, arms races, and hostile relations between states.[13] Governments can make predictions about which states have peaceful or aggressive intentions, but the costs of guessing wrong are high.

Better information about other states' intentions and preferences would allow decision makers to not always assume the worst and pay the high price of that assumption.[14] Arming against a nonexistent or minimal threat is an expensive proposition that diminishes a nation's long-term power by diverting resources to less productive purposes. Thus, many political scientists think this dilemma would not occur if governments knew the intentions of other governments. Uncertainty is an essential element that transparency could take away. Without uncertainty about how other states will use their military power, "the security dilemma is no dilemma and the search for security leads to peace, not war."[15] Treating other governments as enemies can also be a self-fulfilling prophesy if that defensive action provokes a like response.

Yet, resolving this dilemma is difficult because governments have an incentive to misrepresent their preferences.[16] Governments that are truly aggressive may not want to be branded as such and accept all the costs that label brings. Or, governments may simultaneously negotiate and prepare an attack in case negotiations fall through. In this circumstance, they will be loath to share information that will curtail their military options if war becomes necessary.[17]

Moreover, even if transparency accurately shows that a government's intentions are peaceful, there is always a risk that those intentions can change. John Mearsheimer's assertion that "states have little choice but to fear each other" is overly stark but contains a grain of truth.[18] Superior power is often threatening regardless of intentions because governments change, circumstances change, and latent power can always be mobilized. This fact is particularly important because defense planning and procurement must often be years, if not decades, ahead of current needs. Nonetheless, preparations for possible future wars can ultimately reduce security further because such preparations are usually observable and encourage other states to behave likewise.[19]

Transparency may not significantly reduce violent conflicts for the simple reason that not all, or perhaps even most, conflicts are caused by misunderstandings.[20] States also have conflicting interests, which may only get worse if differences are illuminated.[21] Leaders may choose war as a rational or necessary means of resolving those conflicts. Some values are worth fighting for, and violence sometimes may be the only way to protect them.[22]

In addition to failing to stop conflicts, transparency can actually make conflicts worse when it emphasizes truly hostile intentions held by governments or their people. When states actively seek to maximize their power, attempt to expand their territory, or are otherwise greedy or aggressive, transparency is no help.[23] It can act as a megaphone that amplifies hostile rhetoric that can build on itself and reduce the number of politically acceptable options short of the use of force. Transparency and nationalism may be a particularly dangerous mix, especially if that nationalism is motivated by hostile feelings toward some "out-group" or if nationalists view compromise or retreat as a stain on national honor.[24] In either circumstance, transparency may only constrain the options of negotiators and limit the political space available for cooperation.

The 1898 Fashoda Crisis, which began when French and British forces met in the Upper Nile Valley, provides an example of how transparency can amplify hostile intentions in conflicts between democracies. Though tensions were high throughout the crisis and war seemed possible, neither government wanted war. Diplomats worked behind the scenes to resolve the conflict but, in public, politics trumped moderation. French Foreign Minister Delcassé, for instance, was willing to cut a deal privately but spoke "brave words . . . for public consumption." These words were so convincing that the British ambassador to Paris argued that Delcassé believed his own rhetoric and was unwilling to negotiate. The press and parliaments on both sides echoed the belligerent tone. A headline in the French newspaper *Le Matin* read, "The only answer worthy of France is No!" Though the British press generally advocated restraint at the beginning of the standoff, it became increasingly hostile as weeks passed. In France, public opinion grew more pugnacious and the parliament and press picked up this tone. The crisis finally ended when France, the far weaker state in the standoff, chose a humiliating withdrawal over war. Transparency created more room for misperceptions between policy makers in Britain and France because the press and parliaments

on both sides exacerbated hostilities, creating a vicious cycle of action and reaction. Negotiators were able to avoid war only by insulating themselves from public opinion and quietly reaching a decision based on their complex interests.[25]

Domestic politics gives leaders additional incentives to be suspicious and uncooperative in international affairs. To avoid perceptions of weakness or ineffectiveness, leaders may assume the worst when analyzing the behavior of other states, which further reinforces incentives to be suspicious and uncooperative. Under conditions of uncertainty, the political costs of guessing wrong may appear higher than the political rewards of guessing correctly. Politicians do not want to underestimate a threat only to look unprepared later, see their nation victimized by a foreign government due to insufficient capacity to respond, make a cooperative gesture that is not reciprocated, or comply with an international agreement and then find others have cheated. They may also score political points by playing on the xenophobia of citizens. Such behavior is evident in both democracies, where politicians risk being voted out of office, as well as authoritarian regimes, where the costs of being wrong can be far more severe.

Because democracies typically are the most transparent states, they may also send the most belligerent signals when roused. Democracies do not usually fight each other, but strong evidence indicates that democracies fight wars at least as much as other types of states. Classical liberals like Immanuel Kant failed to predict this phenomenon, believing that governments ruled by the people whose lives and treasure would be lost by war, would be the most pacific of nations.[26] But, historically, war is often popular in democracies. Publics may support war even more than their governments, thus constraining efforts at peaceful resolution of a conflict.[27] One of the most cited examples of a popular war by a democracy is the Spanish-American War of 1898, but even the Vietnam War—a war ultimately viewed as a defeat by the United States—received support from a majority of the American public until well into the conflict. Among democracies, democratizing states may be the most dangerous of all. When publics are able to express nationalism that authoritarian regimes suppressed, the results may be a more aggressive foreign policy.[28]

Whereas the case of the Spanish-American War exemplifies how transparency can fuel a crisis, the 2001 EP-3 incident is an example of how a lack of transparency can slow the escalation of crises. On April 1, 2001, an American EP-3E Aries II surveillance plane collided with a Chinese interceptor plane over the South China Sea and crash-landed on Hainan Island in China. All twenty-four crew members survived, but the Chinese government detained them eleven days for questioning. A Chinese pilot, Wang Wei, died in the incident and was declared a national hero by Chinese President Jiang Zemin.[29] In the ensuing crisis, negotiators disputed which plane caused the crash, which side was responsible for the Chinese pilot's death, whether the United States was justified in running surveillance flights in what it claims was international airspace off the Chinese coast, and whether and how the aircraft should be returned. A carefully worded apology by the United States ended the crisis.[30]

Based on traffic at Chinese websites and chat rooms, the Chinese public was incensed at the incident and—already angry at the United States for the accidental bombing of the Chinese embassy in Belgrade—seemed to prefer a harder line than that held by their government. In order to keep a lid on the crisis, the Chinese government allegedly censored the most vociferous critics of both the United States and the Chinese government's handling of the situation. According to executives at a major Internet company in China, Internet service providers deleted a huge number of comments viewed as too critical of the government and a smaller number deemed too supportive of the United States.[31]

A freer flow of information in China might also have produced more ways to express anger at the United States and therefore more ways to build political support for policies that could lead to conflict. Though the government-controlled press is certainly capable of stoking nationalist sentiments, the most jingoistic statements in the press are often found in private, profit-seeking publications and not state-sponsored publications.[32] Unfortunately, the tendency for private media to strike a nationalist or jingoistic tone in order to sell advertisements or papers is not confined to democratizing or authoritarian societies.

Though government censorship is unacceptable to anyone who believes in freedom of speech, it may have helped to defuse the crisis.[33] If stridently nationalist Chinese opinions continued to flourish and became more widely known in the United States, a diplomatic solution could have been that much more complicated.[34] This statement does not suggest such censorship is legitimate or right—it is not. However, it illustrates the complex relationship between transparency, information, and conflict and calls into question ideas that openness alone will encourage more peaceful international relations.

TRANSPARENCY OF CAPABILITIES

States only fight wars they think they can win, according to the scholar Geoffrey Blainey and his many disciples.[35] Clarity about the distribution of state power should facilitate peace. Leaders weigh the costs and benefits of using force and attack when the rewards outweigh the costs. In this calculation, uncertainty about other states' military capabilities can lead them to fight wars they would otherwise avoid. When they have accurate information about the military capabilities of potential rivals, wars often will be unnecessary or unlikely. States normally avoid fighting stronger states since there is no point wasting lives and treasure if they know they are going to lose. Wars with weaker states may be unnecessary because less powerful countries often will comply with stronger states' demands rather than suffer the costs of war.

Deterrence theory is based on the idea that states will avoid fighting wars if they see the costs of war outweigh the benefits.[36] However, the impact of transparency on deterrence depends on whether uncertainty about military capabilities breeds aggression or restraint. Many analysts assume the latter and, consequently,

believe transparency will increase international security by reducing uncertainty. In fact, transparency either supports or undermines deterrence depending on the military capabilities and intentions uncertainty conceals.[37]

Advocates of arms transparency, the sharing of information regarding military capabilities, assume transparency will reduce misperceptions and help countries avoid war. That view may be correct, as long as transparency reveals stability or that the costs of war are unacceptably high. If greater transparency exposes vulnerability, it can undermine deterrence and invite aggression by the strong against the weak. When using force seems easy, strong states have more incentives to use it in order to achieve their goals. Less uncertainty about military capabilities makes strong states more confident of success in war and removes the strategic ambiguity that protects the weak. The effects of transparency depend on what transparency reveals.

The link between arms transparency and peace is complicated further by the fact that many weapons are difficult to classify as unambiguously offensive or defensive and give no clear indication as to strategy.[38] Many weapons, such as small arms, can be used for either offensive or defensive purposes. The best defense against offensive weapons like tanks is strike aircraft and more tanks, both of which are classic offensive weapons.[39] Meanwhile, so-called defensive weapons—like advanced sensors, which provide early warning of conflicts and reduce the chance of surprise attack—can be used in offensive attacks. As Jasjit Singh explains, "Israel used airborne early warning systems, electronic intelligence systems, and precision-guided munitions in an integrated manner to defeat Syria in the Beqa'a Valley in June 1982. Open-source information as well as intelligence made the international community well aware of the type and number of Israeli systems (such as the E-2C), but most observers did not predict the way they were used or the effects of their use."[40]

Recognizing that transparency can both strengthen and undermine deterrence is an important first step toward understanding the implications of greater transparency for international security, but the effects of greater transparency are more complex still. As analysts, we must predict the effects of greater transparency based not only on a snapshot of military capabilities but also on trends.[41] After all, transparency of military capabilities reveals not just how powerful states are, but how powerful they are becoming relative to other states. When less uncertainty leads governments to conclude that power shifts are not in their favor and windows of opportunity are closing, less uncertainty does not encourage restraint. In such circumstances, states feel pressure to act before it is too late, especially if that action will augment their power. States also may strike first to capitalize on the element of surprise. As Bruce Bueno de Mesquita observes, in this scenario "war can begin, even with full information if it is motivated by a fear of ceding any advantage, however small, that is attached to the first use of force."[42]

If states are sufficiently hostile toward one another, deterrence can fail even if capabilities are completely transparent. To give a particularly striking example, during the 1947–48 partition of India and Pakistan, the military assets of the two

newly independent countries were almost completely transparent while a joint commission divided the military assets according to a 2:1 ratio. Personnel on both sides served in the British Indian military in World War II and continued to serve together until August 15, 1947. However, this deep knowledge of the enemy's capabilities did not prevent Pakistan from launching a war a few weeks later—even as the Indo-Pakistan Military Commission, charged with dividing the assets, continued its work.[43]

Arguments regarding deterrence also will not hold if the political costs of peace are higher than the political costs of war. Cost-benefit analyses often assume war is the most costly and undesirable outcome of any conflict and that states will therefore prefer other outcomes. But, historically, that assumption has not always proved accurate. Sometimes weaker states prefer violent loss to surrender because of the political or psychological costs of peaceful surrender. The 1973 Arab-Israeli war is the classic example of this scenario. Egypt attacked though its leaders knew full well Egypt would lose a war against Israel. However, the political victory gained by launching the attack appeared to have compensated for the military loss.

States benefit unequally from military transparency. How states react to less uncertainty in the world depends on how strong they are. In many ways, transparency benefits the strong because it broadcasts that strength and discourages others from attacking. For this reason, it is unsurprising that strong states are more likely to participate in arms transparency regimes than weak states.[44] For weaker states, ambiguity provides a shield that transparency takes away.[45] If, as David Singer argues, "ambiguity and uncertainty is what inhibits escalatory behavior," ambiguity may provide a security advantage for weak states because aggressors may be unsure about the extent or quality of a weak state's military capabilities.[46] Moreover, if weak states can convince potential aggressors that they have a "secret weapon," such as nuclear, biological, or chemical weapons, that potential threat may deter stronger states, even if that threat is obscure. Bluffing in this way can be quite effective as long as the adversary believes there is some probability the state will carry out the threat.[47]

If transparency takes away weak states' leverage, the clear strategy for weak states is to eliminate the need to bluff. And, in today's climate, the way for a weak state to quickly and cheaply increase its bargaining power is to acquire weapons that are so destructive or disturbing that they deter even states with significantly greater military power. Along with Iran, a disturbing example of this is North Korea, which first pursued nuclear weapons clandestinely but increasingly seeks to demonstrate their purported capabilities. As one Bush administration official put it, "What worries us most is that there is a progression of openness among the North Koreans about their nuclear capabilities. They have unfolded new phases of specificity about what they can do and they seem to have been on a long-term path of ending the ambiguity about their capability."[48]

The example of North Korea illustrates that, ultimately, the impact of greater transparency depends not just on the nature of the information but whom that

information is about. Mistrust is tightly linked to identity, because identity provides important clues about how a state will behave in the future. Identity, in this way, reduces international uncertainty. For instance, the United States is more worried about North Korea's nuclear capability than Great Britain's nuclear capability not only because it has less information about how North Korea will use its power, but also because the United States trusts Great Britain not to use its nuclear capability to threaten American interests. As one commentator put it, "The real issue all along is what is the North Korean motivation, why are they doing this [developing nuclear weapons] and what do they want [from the U.S.]."[49]

To give another example, despite Indian defense spending increases of 7.8 percent in 2005–6 and 22 percent the year before, American leaders do not perceive India as a threat. In contrast, China's military build-up (reflected in an 11 percent increase in defense spending in 2004), led the Commander of the United States Pacific Command to state, "It's disconcerting to see this buildup, it seems to be more than might be required for their defense . . . it's certainly a cause for concern."[50]

States interpret information in the context of existing political and security relationships. Consequently, though they may have extensive information about military capabilities, they do not necessarily know whether those capabilities are a threat.[51] The United Nations Register of Conventional Arms (UNROCA) is based on the idea that military capabilities indicate aggressive intent and that transparency of these capabilities will discourage aggression. However, because military capabilities must be interpreted, the relationship between weapons and aggressive intent is not as clear as it might seem at first glance. According to the UNROCA framework, governments should be concerned when arms acquisitions are "excessive and destabilizing." But what exactly does "excessive and destabilizing" mean? Threats are often in the eye of the beholder and definitions, no matter how complex, cannot fully respond to these perceptions. Governments continue to disagree about the number and kinds of weapons, doctrines, and strategies needed to deter an adversary. With no generally accepted answer to the question of how much deterrence is enough, even military power designed to deter and not to conquer can be interpreted as evidence of aggressive intentions.

In short, transparency of military capabilities alone is often not sufficient to transform states' national security behavior.

KNOWING OTHERS BETTER

The idea that knowledge of others will reduce international conflict is widely held. By spreading information about different nations and peoples, global transparency is expected to increase understanding of others, humanize them, and reduce the desire for violence. By giving people access to many different sources of information, greater transparency is also expected to create a "marketplace of

ideas" that prevents leaders from monopolizing channels of communication and demonizing other groups.[52] Greater transparency, optimists argue, will reduce conflicts because monopolies over information are necessary in order to dehumanize other groups sufficiently to justify violence against them; a free marketplace of ideas has a "self-righting tendency to correct errors and biases."[53]

Yet, the effects of transparency are more complex than these views suggest. Greater transparency *can* increase positive feelings between groups by spreading knowledge of other groups and increasing contact between them. But when these circumstances do not exist, transparency can be dangerous. When transparency exposes competing values or entrenched hostility, or it undermines established social allegiances, the trend toward greater transparency may exacerbate conflicts. Depending on what transparency shows, greater transparency can spread information that dehumanizes others rather than humanizes them or makes people realize they abhor the values of others, not share them.[54]

To overcome intergroup suspicion, studies indicate that more contact increases positive feelings toward other groups only under certain conditions, the two most important of which are that the groups have equal status and share common goals. When that is not the case, contact can increase negative feelings toward those groups.[55] Research shows that increased contact also exacerbates hostility when there are significant differences—whether cultural, ethnic, social, or political—between groups or institutionalized preferential treatment for one group over another. If greater transparency exposes these differences, it may increase the likelihood of conflict. According to Yale University law professor Amy Chua, such intergroup differences are particularly likely to create hostility when a minority group controls the vast majority of an area's wealth. This situation can create violent backlash against the minority group, especially during transitions to democracy and free markets, within a single country or in the global context. Chua believes that hostility toward Chinese in Southeast Asia and Tutsis in Rwanda is analogous to widespread hatred of Americans, who control a disproportionate share of global wealth.[56]

Increasing transparency may raise awareness of extremist groups and their messages among mass audiences and, possibly, increase the power of those groups. When new political groups are competing for power in a society, growing transparency may encourage groups to stake out more extreme, black-and-white positions that separate them from their opponents. In a fluid and boisterous political climate, transparency may only encourage the press, opposition parties, the government, or civil society to see who can voice their views the loudest, regardless of how hostile they are. In such climates, incomplete transparency may provide exposure for new ideas but not enough information to counter false claims.[57]

Many argue that truth will win if information flows freely and creates a "marketplace of ideas." However, that view is based on the assumption that, in the marketplace, people are shopping for truth. If instead they are shopping for self-esteem and view the degradation of out-groups as increasing self-esteem, the

marketplace of ideas, sadly, will not function as classical liberals like Mill intended. A marketplace of ideas also may not encourage tolerance if people do not re-examine their views when confronted with evidence that contradicts them. In such circumstances, prejudice is independent of whether negative stereotypes are false.[58] For reasons ranging from self-esteem to the human tendency to minimize cognitive dissonance, people may distrust or disregard information that did not fit with their previously held beliefs.[59] For example, after viewing a 2001 videotape of Osama bin Laden in which bin Laden seemed to laugh at the September 11th attacks, some Arabs, convinced bin Laden is a holy man, argued the tape was a fake.[60]

A related danger is that the marketplace of ideas produces such a plethora of ideas that citizens pay attention only to information that confirms their existing views, a phenomenon justified by empirical evidence.[61] In the information age, people have even more opportunities to pick and choose information that supports their views or find and surround themselves with like-minded people. Hundreds of thousands of groups have their own web pages, blogs, or social networks that are facilitated by the Internet.[62] By protecting themselves from having to defend their views, people can avoid the cognitive discomfort of needing to change their beliefs.

Any doubt that global transparency has a dark side should be laid to rest by the violence that followed publication of cartoons perceived as offensive by many Muslims. Much protest of those cartoons was peaceful, but some erupted into violence. The episode began in September 2005 when a Danish newspaper called *Jyllands-Posten* published twelve cartoons that unsympathetically depicted the prophet Mohammed and satirically linked Islam to terrorism. Muslim leaders in Denmark protested but at first generated little reaction. In December 2005 groups of these leaders traveled to Lebanon, Syria, and Egypt, where a news conference gained wide coverage in the Arabic-language media.[63] Though initial reaction to the cartoons was slow, the first spark soon spread like wildfire. Muslims from around the world, in Indonesia and the United Kingdom and the Middle East, e-mailed each other, posted the cartoons on websites, and discussed their outrage in Internet chat rooms. Using all the tools of electronic communication, they organized a boycott of Danish products. This eruption made the cartoons newsworthy again, leading the German newspaper *Die Welt* to publish a story about the controversy and also reprint nine of the cartoons. An Italian newspaper, *the Corriere*, reprinted three of the cartoons along with three anti-Semitic cartoons reprinted from Arab newspapers and three Nazi-era propaganda posters.[64] Protests broke out on February 3rd in Indonesia, Malaysia, the Palestinian territories, and Iraq, and were soon followed by attacks on embassies and mass protests in Lebanon, Syria, Iran, Pakistan, Afghanistan, Nigeria, Europe, and North America. Some of those protests—in Afghanistan, Libya, Nigeria, and Pakistan—turned violent, leaving forty-three dead by month's end.[65]

Throughout the protests, images of both the cartoons and the protests spread around the world via satellite television, the Internet, and newspapers. These

images reported the story, spreading legitimate dissent as well as incitement to violence. Transparency spread news about the cartoons, reaction to them, and truthful opinion. It also spread misinformation, hatred, and incited calls for violence. Transparency facilitates the spread of truth and falsehood, peace and violence alike.

INTELLIGENCE IN THE AGE OF TRANSPARENCY

What are the implications of global transparency for national intelligence? First, with respect to collection, global transparency means that there is a virtual torrent of open-source information, which is both a treasure and a curse. We can learn a tremendous amount about other societies simply by reading their newspapers, unclassified documents, and the publications of nongovernmental organizations (NGOs) that ferret out information and analyze it. But the sheer volume of information available from open and covert sources does not mean that intelligence agencies have all the information they need. Indeed, certain types of information are particularly valuable in the age of transparency. Intentions (i.e., what will actors do with the resources they have, what do they intend to do in the future, are those intentions in line with or counter to one's own national interests?) are one such area. Another useful area for intelligence collection is to find out what information sources publics and leaders turn to, what sources they trust, and how they interpret information in that light. That understanding will help prediction because it facilitates the ability to put oneself in another's shoes.

Analysis is the area of intelligence most complicated by global transparency. There is simply so much information to evaluate that deriving meaning can be like finding a needle in a haystack. Studies show that people are likely to be more successful in recognizing the "truth" if the "signal-to-noise" ratio—i.e., the strength of the signal relative to the strength of the confusing or distracting background stimuli—is low. When there is simply too much information—a significant risk in an age of transparency—people may disregard important data.[66] For instance, according to Astri Suhrke and Bruce Jones, cognitive factors contributed to the world's failure to recognize an impending genocide in Rwanda. The situation was complex and difficult to understand amid the "noise" and propaganda coming out of Kigali. Consequently, observers interpreted raw information differently. Some diplomats thought the violence originally was directed against political opponents of the government and were not prepared for the genocide. Others thought the Tutsis were at great risk. Still others saw hate propaganda as a tool to exert pressure for political concessions. Even Tutsi leaders often underestimated the threat. As one Tutsi leader later explained, "What they said was so stupid; we did not take it seriously enough."[67]

Analysts will also need to avoid analytical errors caused by inaccurate understandings of transparency's complex effects. As indicated in this chapter, much of the conventional wisdom regarding transparency is either wrong or

conditional. Understanding when conventional theories of transparency will hold, and conditions under which they will not, may help analysts to make better predictions.

Covert action is a third area of intelligence complicated by global transparency. Intelligence agencies must face the reality that any covert act could become public, a fact that significantly affects the cost-benefit analysis when considering covert action. A particular covert action could have a net positive effect if it stays clandestine, but the negative costs to that action becoming public could outweigh that benefit in many circumstances. Some public diplomacy experts, for instance, questioned the United States' alleged use of secret prisons to hold detainees in Europe. Though those prisons undoubtedly were useful to American intelligence agencies, the resulting public firestorm in Europe could curtail seriously the United States' room for action in the future. Decision makers must weigh when tactical gains risk losing the war and when those gains are worth the price.

CONCLUSION

Global transparency will benefit the world in many ways. It is likely to make governments less corrupt, more accountable, and more responsive to their citizens. In the realm of international security, transparency can reduce misperceptions and help governments to see when they and their neighbors want peace. However, global transparency will not necessarily lead to peace and in many ways it makes national security policy, and therefore national intelligence, more complex. Transparency can undermine deterrence, spotlight and spread hostility, and encourage vicious cycles of belligerent rhetoric and actions. Instead of showing information that enhances security, transparency sometimes can undermine it.

Because the effects of transparency are so complicated, we must analyze carefully where people look for information, what information transparency reveals, how people interpret that information, what sources of information people trust, and what reactions to information people find legitimate and appropriate. These factors play a critical role in international politics and security. For that reason, they must also be critical to national intelligence agencies. In an age of transparency, collecting information is difficult. Understanding it is even harder.

NOTES

1. See Freedom House's list of electoral democracies for 2005 at http://www.freedomhouse.org/template.cfm? page+2005&year=2005.

2. For elaboration of this argument, see Kristin M. Lord, *Perils and Promise of Global Transparency* (Albany: SUNY Press, 2006), and Bernard I. Finel and Kristin

M. Lord, eds., *Power and Conflict in the Age of Transparency* (New York: Palgrave Macmillan, 2000).

3. See Finel and Lord, eds., *Power and Conflict in the Age of Transparency*. This definition is similar to that offered by Antonia Handler Chayes and Abram Chayes in their work on international regimes: "Transparency is the availability and accessibility of knowledge and information" regarding international regimes, their policies, and the activities of their parties. See Chayes and Chayes, "Regimes Architecture: Elements and Principles," in *Global Engagement: Cooperation and Security in the 21st Century,* ed. Janne E. Nolan (Washington, DC: Brookings Institution, 1994), p. 81.

4. On this point, see Charles Lipson, *Reliable Partners: How Democracies Have Made a Separate Peace* (Princeton: Princeton University Press, 2003).

5. Social practices reduce uncertainty. For a discussion, see Nicholas Greenwood Onuf, *World of Our Making: Rules and Rule in Social Theory and International Relations (Studies in International Relations)* (Columbia: University of South Carolina Press, 1989).

6. Reported in Barbara Amiel, "Is the Muslim World Still in Denial About September 11?" *Daily Telegraph* (March 4, 2002), p. 20.

7. David Hoffman, "Beyond Public Diplomacy," *Foreign Affairs* (March/April 2002), p. 83.

8. David J. Finlay, Ole R. Holsti, and Richard R. Fagen, *Enemies in Politics* (Chicago: Rand McNally, 1967), p. 15.

9. Andrew Kydd, "Trust, Reassurance, Cooperation," *International Organization* 54 (Spring 2000), p. 341.

10. Quoted in Bruce Russett, *Grasping the Democratic Peace: Principles for a Post-Cold War World* (Princeton: Princeton University Press, 1993), p. 127.

11. Michael Barnett, "Institutions, Roles and Disorder: The Case of the Arab State System," *International Studies Quarterly* (September 1993); also Michael Barnett, "Sovereignty, Nationalism and Regional Order in the Arab System," *International Organization* 49 (Summer 1995).

12. See Thomas Schelling, *Strategy of Conflict*; Robert Axelrod, *Evolution of Cooperation* (New York: Basic Books, 1984); Charles L. Glaser, "The Security Dilemma Revisited," *World Politics* 50 (October 1997).

13. For a discussion of how the security dilemma operates in domestic ethnic conflicts, see Barry R. Posen, "The Security Dilemma and Ethnic Conflict," *Survival* 35 (Spring 1993).

14. Andrew Kydd, "Sheep in Sheep's Clothing," *Security Studies* (1997), p. 125.

15. Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30 (January 1978), p. 126.

16. James D. Fearon, "Rationalist Explanations for War," *International Organization* 49 (Summer 1995), p. 381.

17. David A. Lake and Donald Rothchild, "Containing Fear: The Origins and Management of Ethnic Conflict," *International Security* 21 (Fall 1996), pp. 46–47.

18. John Mearsheimer, "The False Promise of International Institutions," *International Security* (Winter 94/95). For a discussion of the tragic nature of realist thought, see Michael Spirtas, "A House Divided: Tragedy and Evil in Realist Theory," *Security Studies* 5 (Spring 1996).

19. Iraq, which the United States government actively supported for many years, is an example of how a regime can be considered a friend at one time and a foe later, even when the country's leadership stays the same.

20. For a related argument, see Randall Schweller, "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies* 5 (Spring 1996), and "Bandwagoning for Profit: Bringing the Revisionist State Back In," *International Security* 19 (Summer 1994). Schweller rightly notes that not all states are interested in security alone. Governments are also motivated by desires for territory, influence, power, wealth, and so on.

21. Ann Florini, *The Coming Democracy: New Rules for a New World*, (Washington, DC: Island Press, 2003).

22. Janne Nolan, ed., *Global Engagement: Cooperative Security in the 21st Century* (Washington, DC: Brookings, 1994), p. 4.

23. This view is ascribed to "classical" realists such as Hans Morgenthau. See Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, 6th ed. (New York: Knopf 1985).

24. Ernst Haas defines nationalism as a "doctrine of social solidarity based on the characteristics and symbols of nationhood." A nation is a "socially mobilized body of individuals who believe themselves united by some set of characteristics that differentiate them (in their own minds) from outsiders and who strive to create or maintain their own state." See Ernst B. Haas, *Nationalism, Liberalism and Progress: The Rise and Decline of Nationalism*, Vol I. (Ithaca: Cornell University Press, 1997), p. 23.

25. See P. Wright, *Conflict on the Nile: The Fashoda Incident of 1898* (London: Heinemann, 1972), pp. 44–45. Quoted in Darrell Bates, *The Fashoda Incident of 1898: Encounter on the Nile* (London: Oxford University Press 1984), p. 153. See T. W. Riker, "Survey of British Policy in the Fashoda Crisis," *Political Science Quarterly* 44 (1929), p. 66; R. G. Brown, *Fashoda Reconsidered: The Impact of Domestic Politics on French Policy in Africa 1893–1898* (Baltimore: Johns Hopkins University Press, 1970), p. 112; William F. Hoeft Jr. "Explaining the Interdemocratic Peace: The Norm of Cooperatively Biased Reciprocity," Ph.D. dissertation, Georgetown University (May 18, 1993), pp. 312–22, 396.

26. See Immanuel Kant, *Perpetual Peace* (New York: Columbia University Press, 1939). For an excellent analysis of the democratic peace, see James Lee Ray, *Democracy and International Conflict: An Evaluation of the Democratic Peace Proposition* (Columbia: University of South Carolina Press, 1995).

27. John M. Owen, "How Liberalism Produces Democratic Peace," *International Security* (Fall 1994), p. 91.

28. See Harry Harding in Ezra Vogel, ed., *Living with China: US-China Relations in the Twenty-First Century* (New York: Norton, 1997), p. 176. See also Edward Mansfield and Jack Snyder "Democratization and the Danger of War," *International Security* 20 (Summer 1995), and Bruce Russet, *Controlling the Sword: The Democratic Governance of National Security* (Cambridge: Harvard University Press, 1990).

29. Clay Chandler, "U.S. May Quit Talks With China Over Plane; Beijing Is Pressed to Discuss Return of Damaged Aircraft," *Washington Post* (April 19, 2001), p. A1. See also Thomas L. Friedman, "Myth-Matched Nations," *New York Times* (April 17, 2001), p. A19; Frank Langfitt, "China Launches Battle for Public Opinion: Regime Tries to Sell Deal on U.S. Aircrew," *Baltimore Sun* (April 13, 2001), p. 1A.

30. The word "apology" was not used in the official letter. Instead, President Bush wrote that the United States was "very sorry" for the pilot's death and the EP-3E's unauthorized emergency landing on Chinese territory and expressed "sincere regret" over the incident.

31. Elisabeth Rosenthal, "Collision With China: Reaction in China; Beijing Declares Victory but Chat Rooms Are Skeptical," *New York Times* (April 13, 2001), p. 11.

32. See Kristof, April 22, 2001.

33. See Craig S. Smith, "Chinese Youths' Darkening View of U.S.," *New York Times* (April 22, 2001), p. 6.

34. According to Richard Worf, the Chinese government set up anti–United States Internet chat rooms and did not publicize President Bush's initial statement of regret. See Richard Worf, "Speaking Out: The Internet in China," *Harvard International Review* (Winter 2002), pp. 7–8. See also Elisabeth Rosenthal, "Collision With China: Reaction in China; Beijing Declares Victory but Chat Rooms Are Skeptical," *New York Times* (April 13, 2001), p. A11; Oliver August, "Internet Censors Cut the Chinese Chat," *The Times* (April 13, 2001); David Rennie, "Chinese Feel Betrayed by 'Double Meaning,' " *Daily Telegraph* (April 12, 2001), p. 16; Mark O'Neill, "Anti-U.S. Fervour Pours Into Chat Rooms," *South China Morning Post* (April 8, 2001), p. 11; John Pomfret, "New Nationalism Drives Beijing; Hard Line Reflects Public Mood," *Washington Post* (April 4, 2001), p. A1.

35. See Geoffrey Blainey, *The Causes of War* (New York: Free Press, 1973). See also Richard Ned Lebow, *Between Peace and War* (Baltimore: Johns Hopkins University Press, 1981).

36. Jasjit Singh, "The UN Register: Transparency and the Promotion of Conflict Prevention and Restraint," in Chalmers, et al., *Developing Arms Transparency* (1997), p. 135. See also F. S. Pearson and M. Brzoska, *Arms and Warfare: Escalation, Deescalation, Negotiation* (Columbia: University of South Carolina Press, 1994).

37. The effects of transparency also depend on the risk propensities of leaders. If leaders are more likely to accept risk, uncertainty can tempt them to gamble and risk provoking a conflict. If leaders are risk-averse, uncertainty may encourage caution. For a discussion, see Paul Huth, D. Scott Bennett, and Christopher Gelpi, "System Uncertainty, Risk Propensity, and International Conflict Among the Great Powers," *Journal of Conflict Resolution* 36 (September, 1992), p. 488.

38. Catherine M. Kelleher, "Indicators of Defensive Intent in Conventional Force Structures and Operations in Europe," in *Military Power in Europe,* ed. Lawrence Freeman (New York: St. Martin's Press, 1990); and The Palme Commission Report in *Common Security: A Programme for Disarmament*, Report of the Independent Commission on Disarmament and Security Issues (London: Pan Books, 1983); Jonathan Dean, "Alternative Defense: Answer to NATO's Central Front Problems," *International Security* 54 (1988). See also Robert Jervis, "Arms Control, Stability and the Causes of War," *Political Science Quarterly* 108 (1993).

39. Kelleher, "Indicators of Defensive Intent in Conventional Force Structures and Operations in Europe," in *Military Power in Europe,* ed. Freeman, p. 166.

40. Singh, "The UN Register," in Chalmers, et al., *Developing Arms Transparency* (1997), p. 132.

41. For an excellent discussion of the global implications of the rise and decline of state power, see Robert Gilpin, *War and Change in World Politics* (Cambridge, MA: Cambridge University Press, 1981).

42. Bruce Bueno de Mesquita and David Lalman, *War and Reason* (New Haven: Yale University Press, 1992), p. 250.

43. Singh, "The UN Register," in Chalmers, et al., *Developing Arms Transparency* (1997), p. 136.

44. For empirical evidence to this effect, see James H. Lebovic, "Open to Inspection: Democracies and Transparency in the Conventional Arms Trade," unpublished paper.

45. Singh, "The UN Register," in Chalmers, et al., *Developing Arms Transparency* (1997), p. 130.

46. J. David Singer, "System Structure, Decision Processes, and the Incidence of International War," in *Handbook of War Studies,* ed. Manus I. Midlarsky (Boston: Unwin Hyman, 1989), p. 6.

47. See Schelling, *Strategy of Conflict*.

48. David E. Sanger, "U.S. Warns North Korea Against Nuclear Test," *New York Times* (May 7, 2005), p. A9.

49. Quoted in Murray Hiebert, "The North Korea Mystery," *Far Eastern Economic Review* (October 21, 2004), p. 21.

50. Thanks to Harry Harding for this comparison. See John Ruwitch, "China to Boost Military Spending as It Eyes Taiwan," DefenseNews.com (February 28, 2005; accessed June 24, 2005); Nathan Hodge, "New Pacific Commander Sees 'Disconcerting' China Buildup," *Defense Daily International* (March 11, 2005), p. 1; Siddharth Srivastava, "India's Military Hungry for More," *Asia Times* (February 16, 2005), available at http://www.atimes.com (accessed June 24, 2005); Pulkit Singh, "Indian Defense Budget Rises 7.8% to $19B," *Journal of Electronic Defense* (April 2005), p. 19.

51. On the trade-off between military capabilities and policy intentions in assessing threat, see J. David Singer, "Threat Perception and the Armament-Tension Dilemma," *Journal of Conflict Resolution* (March 1958).

52. Susan Carruthers, *The Media at War* (London: Macmillan, 2000), p. 44. See also Ervin Staub, "Individual and Group Identities in Genocide and Mass Killing," in Richard D. Ashmore, Lee Jussim, and David Wilder, eds., *Social Identity, Intergroup Conflict, and Conflict Reduction* (Oxford: Oxford University Press, 2001), pp. 177–78.

53. David Kelley and Roger Donway, "Liberalism and Free Speech," in *Democracy and the Mass Media,* ed. Judith Lichtenberg (Cambridge: Cambridge University Press, 1990), p. 90.

54. The need to dehumanize enemies in order to justify violence may explain why societies with free presses do not fight each other. Free presses offer citizens competing interpretations of government policy and humanize the "other." Democracies protect minority rights and typically feature a marketplace of ideas that can refute prejudice. See Douglas A. Van Belle, *Press Freedom and Global Politics* (Westport, CT: Praeger, 2000).

55. See H. D. Forbes, *Ethnic Conflict: Commerce, Culture, and the Contact Hypothesis* (New Haven: Yale University Press, 1997). See also Gordon Allport, *The Nature of Prejudice* (Reading, MA: Addison-Wesley, 1954), and Thomas F. Pettigrew, "Intergroup Contact Theory," *Annual Review of Psychology* 49 (1998).

56. Amy Chua, *World on Fire: How Exporting Free Market Democracy Breeds Ethnic Hatred and Global Instability* (New York: Anchor Books, 2003).

57. Ironically, the very institutions that are supposed to create a balanced and diverse marketplace of ideas sometimes promote intolerant discourse. The media can air

hatred toward out-groups and legitimate violence—particularly if that sort of coverage has an avid audience and sells newspapers. Democracies and their citizens sometimes embrace prejudice or war. Laws that encourage a marketplace of ideas, such as freedom of speech, can provide "an opening for nationalist mythmakers to hijack public discourse." See Jack Snyder and Karen Ballentine, "Nationalism and the Marketplace of Ideas," *International Security* (Fall 1996). Civil society can include extremist and terrorist groups as well as groups that advocate civil and human rights. See also Larry Diamond, "Rethinking Civil Society: Toward Democratic Consolidation," *Journal of Democracy* 5 (September 1994).

58. Forbes, *Ethnic Conflict*, p. 168.

59. See, for instance, Robert Jervis, *Perception and Misperception in International Politics* (Princeton: Princeton University Press, 1976).

60. Daniel Drezner and Henry Farrell, "Web of Influence," *Foreign Policy* (November/December 2004).

61. The "selective exposure hypothesis," also known as defensive avoidance, was first associated with Leon Festinger. See his *Conflict, Decision and Dissonance* (Stanford: Stanford University Press, 1964). However, note that successive studies showed that specific factors can offset selective tendency, for example, message's utility, ease of refutability. For a discussion, see Jervis, *Perception and Misperception*, pp. 143–216, and Ole Holsti, "Cognitive Dynamics and Images of the Enemy: Dulles and Russia," in *Enemies in Politics,* eds. David Finley, Ole Holsti, and Richard Fagen (Chicago: Rand McNally, 1976). See also James M. Goldgeier, "Psychology and Security," *Security Studies* 6 (Summer 1997), p. 141; Spillmann and Spillmann, "On Enemy Images and Conflict Escalation" (1991), pp. 72–73.

62. David Hoffman, "Beyond Public Diplomacy," *Foreign Affairs* (March/April 2002), p. 83.

63. Anthony Shadid and Kevin Sullivan, "Anatomy of the Cartoon Protest Movement," *Washington Post* (February 16, 2006), p. A1.

64. Ibid.

65. See BBC News, "Nigeria Cartoons Protest Kills 16," February 19, 2006, available at http://news/bbc.co.uk/1/hi/world/africa/4728616.stm.

66. See Herbert A. Simon, "Information 101: It's Not What You Know, It's How You Know It," *Journal for Quality and Participation* (July/August 1998).

67. Astri Suhrke and Bruce Jones, "Preventive Diplomacy in Rwanda: Failure to Act or Failure of Actions?" in Bruce W. Jentleson, *Opportunities Missed, Opportunities Seized: Preventive Diplomacy in the Post–Cold War World* (New York: Carnegie Commission on Preventing Deadly Conflict, 2000), pp. 254–55.

APPENDIX A

INTELLIGENCE EXCERPTS FROM THE NATIONAL SECURITY ACT OF 1947

NATIONAL SECURITY ACT OF 1947

ACT OF JULY 26, 1947

An act to promote the national security by providing for a Secretary of Defense; for a National Military Establishment; for a Department of the Army, a Department of the Navy, and a Department of the Air Force; and for the coordination of the activities of the National Military Establishment with other departments and agencies of the Government concerned with the national security.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE

That [50 U.S.C. 401 note] this Act may be cited as the "National Security Act of 1947."

TABLE OF CONTENTS

[1] Item editorially inserted.

[2] This section was redesignated as section 108 by section 705(a)(2) of P.L. 102–496, but this entry in the table of contents was not repealed.

[3] Section repealed without amending table of contents.

[4] Section repealed without amending table of contents.

[5] Item editorially inserted.

DECLARATION OF POLICY

Sec. 2. [50 U.S.C. 401] In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future secretary of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the nation security; to provide a Department of Defense, including the three military Departments of the Army, the Navy (including naval aviation and the United States Marine Corps), and the Air Force under the direction, authority, and control of the Secretary of Defense; to provide that each military department shall be separately organized under its own Secretary and shall function under the direction, authority, and control of the Secretary of Defense; to provide for their unified direction under civilian control of the Secretary of Defense but not to merge these departments or services; to provide for the establishment of unified or specified combatant commands, and a clear and direct line of command to such commands; to eliminate unnecessary duplication in the Department of Defense, and particularly in the field of research and engineering by vesting its overall direction and control in the Secretary of Defense; to provide more effective, efficient, and economical administration in the Department of Defense; to provide for the unified strategic direction of the combatant forces, for their operation under unified command, and for their integration into an efficient team of land, naval, and air forces but not to establish a single Chief of Staff over the armed forces nor an overall armed forces general staff.

DEFINITIONS

Sec. 3. [50 U.S.C. 401a] As used in this Act:

(1) The term "intelligence" includes foreign intelligence and counterintelligence.

(2) The term "foreign intelligence" means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons.

(3) The term "counterintelligence" means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

(4) The term "intelligence community" includes—

(A) the Office of the Director of Central Intelligence, which shall include the Office of the Deputy Director of Central Intelligence, the National Intelligence Council (as provided for in section 105(b)(3)), and such other offices as the Director may designate;

(B) the Central Intelligence Agency;

(C) the National Security Agency;

(D) the Defense Intelligence Agency;

(E) the central imagery authority within the Department of Defense;

(F) the National Reconnaissance Office;

(G) other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;

(H) the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, the Department of Treasury, and the Department of Energy;

(I) the Bureau of Intelligence and Research of the Department of State; and

(J) such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of Central Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

(5) The terms "national intelligence" and "intelligence related to the national security"—

(A) each refer to intelligence which pertains to the interests of more than one department or agency of the Government; and

(B) do not refer to counterintelligence or law enforcement activities conducted by the Federal Bureau of Investigation except to the extent provided for in procedures agreed to by the Director of Central Intelligence and the Attorney General, or otherwise as expressly provided for in this title.

(6) The term "National Foreign Intelligence Program" refers to all programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of Central Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

TITLE I—COORDINATION FOR NATIONAL SECURITY

NATIONAL SECURITY COUNCIL

Sec. 101. [50 U.S.C. 402] (a) There is hereby established a council to be known as the National Security Council (thereinafter in this section referred to as the "Council").

The President of the United States shall preside over meetings of the Council: *Provided*, That in his absence he may designate a member of the Council to preside in his place.

The function of the Council shall be to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security.

The Council shall be composed of[6]—

(1) the President;

(2) the Vice President;

(3) the Secretary of State;

(4) the Secretary of Defense;

(5) the Director for Mutual Security;

(6) the Chairman of the National Security Resources Board; and

(7) The Secretaries and Under Secretaries of other executive departments and the military departments, the Chairman of the Munitions Board, and the Chairman of the Research and Development Board, when appointed by the President by and with the advice and consent of the Senate, to serve at his pleasure.

(b) In addition to performing such other functions as the President may direct, for the purpose of more effectively coordinating the policies and functions of the departments and agencies of the Government relating to the national security, it shall, subject to the direction of the President, be the duty of the Council—

(1) to assess and appraise the objectives, commitments, and risks of the United States in relation to our actual and potential military power, in the interest of national security, for the purpose of making recommendations to the President in connection therewith; and

(2) to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security, and to make recommendations to the President in connection therewith.

(c) The Council shall have a staff to be headed by a civilian executive secretary who shall be appointed by the President, and who shall receive compensation at the rate of $10,000 a year.[7] The executive secretary, subject to the direction of the Council, is hereby authorized, subject to the civil-service laws and the Classification Act of 1923, as

---

[6] The positions of Director for Mutual Security, Chairman of the National Security Resources Board, Chairman of the Munitions Board, and Chairman of the Research and Development Board have been abolished by various Reorganization Plans. The statutory members of the National Security Council are the President, Vice President, Secretary of State, and Secretary of Defense.

[7] The specification of the salary of the head of the National Security Council staff is obsolete and has been superseded.

amended,[8] to appoint and fix the compensation of such personnel as may be necessary to perform such duties as may be prescribed by the Council in connection with the performance of its functions.

(d) The Council shall, from time to time, make such recommendations, and such other reports to the President as it deems appropriate or as the President may require.

(e) The Chairman (or in his absence the Vice Chairman) of the Joints Chief of Staff may, in his role as principal military adviser to the National Security Council and subject to the direction of the President, attend and participate in meetings of the National Security Council.

(f) The Director of National Drug Control Policy may, in his role as principal adviser to the National Security Council on national drug control policy, and subject to the direction of the President, attend and participate in meetings of the National Security Council.[9]

(g) The President shall establish with the National Security Council a board to be known as the "Board for Low Intensity Conflict." The principal function of the board shall be to coordinate the policies of the United States for low intensity conflict.

(h) The Director of Central Intelligence (or, in the Director's absence, the Deputy Director of Central Intelligence) may, in the performance of the Director's duties under this Act and subject to the direction of the President, attend and participate in meetings of the National Security Council.

CENTRAL INTELLIGENCE AGENCY

Sec. 102. [50 U.S.C. 403] (a)(1) There is hereby established a Central Intelligence Agency.

(2) There shall be a Director of Central Intelligence who shall be appointed by the President, by and with the advice and consent of the Senate. The Director shall—

(A) serve as head of the United States intelligence community;

(B) act as the principal adviser to the President for intelligence matters related to the national security; and

(C) serve as head of the Central Intelligence Agency.

(b) To assist the Director of Central Intelligence in carrying out the Director's responsibilities under this Act, there shall be a Deputy Director of Central Intelligence, who shall be appointed by the President, by and with the advice and consent of the Senate, who shall act for, and exercise the powers of, the Director during the Director's absence or disability.

(c)(1) The Director or Deputy Director of Central Intelligence may be appointed from among the commissioned officers of the Armed Forces, or from civilian life, but at no time

[8] The Classification Act of 1923 was repealed by the Classification Act of 1949. The Classification Act of 1949 was repealed by the law enacting title 5, United States Code (Public Law 89–544, Sept. 6, 1966, 80 Stat. 378), and its provisions were codified as chapter 51 and subchapter 53 of title 5. Section 7(b) of that Act (80 Stat. 631) provided: "A reference to a law replaced by sections 1–6 of this Act, including a reference in a regulation, order, or other law, is deemed to refer to the corresponding provision enacted by this Act."

[9] The amendment made by § 1003(a)(3) of P.L. 100–690 (102 Stat. 4182), redesignating subsection (f) as (g) and adding a new (f) is repealed by section 1099 of P.L. 100–690 (102 Stat. 4188), effective Nov. 18, 1993.

shall both positions be simultaneously occupied by commissioned officers of the Armed Forces, whether in an active or retired status.

(2) It is the sense of the Congress that under ordinary circumstances, it is desirable that either the Director or the Deputy Director be a commissioned officer of the Armed Forces or that either such appointee otherwise have, by training or experience, an appreciation of military intelligence activities and requirements.

(3)(A) A commissioned officer of the Armed Forces appointed pursuant to paragraph (2) or (3), while serving in such position—

(i) shall not be subject to supervision or control by the Secretary of Defense or by any officer or employee of the Department of Defense;

(ii) shall not exercise, by reason of the officer's status as a commissioned officer, any supervision or control with respect to any of the military or civilian personnel of the Department of Defense except as otherwise authorized by law; and

(iii) shall not be counted against the numbers and percentages of commissioned officers of the rank and grade of such officer authorized for the military department of which such officer is a member.

(B) Except as provided in clause (i) or (ii) of paragraph (A), the appointment of a commissioned officer of the Armed Forces pursuant to paragraph (2) or (3) shall in no way affect the status, position, rank, or grade of such officer in the Armed Forces, or any emolument, perquisite, right, privilege, or benefit incident to or arising out of any such status, position, rank, or grade.

(C) A commissioned officer of the Armed Forces appointed pursuant to subsection (a) or (b), while serving in such position, shall continue to receive military pay and allowances (including retired pay) payable to a commissioned officer of the officer's grade and length of service for which the appropriate military department shall be reimbursed from funds available to the Director of Central Intelligence.

(D) The Office of the Director of Central Intelligence shall, for administrative purposes, be within the Central Intelligence Agency.

RESPONSIBILITIES OF THE DIRECTOR OF CENTRAL INTELLIGENCE

SEC. 103. [50 U.S.C. 403–3] (a) PROVISION OF INTELLIGENCE.—(1) Under the direction of the National Security Council, the Director of Central Intelligence shall be responsible for providing national intelligence—

(A) to the President;

(B) to the heads of departments and agencies of the executive branch;

(C) to the Chairman of the Joint Chiefs of Staff and senior military commanders; and

(D) where appropriate, to the Senate and House of Representatives and the committees thereof.

(2) Such national intelligence should be timely, objective, independent of political considerations, and based upon all sources available to the intelligence community.

(b) NATIONAL INTELLIGENCE COUNCIL.—(1)(A) There is established with the Office of the Director of Central Intelligence the National Intelligence Council (hereafter in this section referred to as the "Council"). The Council shall be composed of senior analysts within the intelligence community and substantive experts from the public and private sector, who shall be appointed by, report to, and serve at the pleasure of, the Director of Central Intelligence.

(B) The Director shall prescribe appropriate security requirements for personnel appointed from the private sector as a condition of service on the Council to ensure the protection of intelligence sources and methods while avoiding, wherever possible, unduly intrusive requirements which the Director considers to be unnecessary for this purpose.

(2) The Council shall—

(A) produce national intelligence estimates for the Government, including, wherever the Council considers appropriate, alternative views held by elements of the intelligence community; and

(B) otherwise assist the Director in carrying out the responsibilities described in subsection (a).

(3) Within their respective areas of expertise and under the direction of the Director, the members of the Council shall constitute the senior intelligence advisers of the intelligence community for purposes of representing the views of the intelligence community within the Government.

(4) The Director shall make available to the Council such staff as may be necessary to permit the Council to carry out its responsibilities under this subsection and shall take appropriate measures to ensure that the Council and its staff satisfy the needs of policy-making officials and other consumers of intelligence.

(5) The heads of elements within the intelligence community shall, as appropriate, furnish such support to the Council, including the preparation of intelligence analyses, as may be required by the Director.

(c) HEAD OF THE INTELLIGENCE COMMUNITY.—In the Director's capacity as head of the intelligence community, the Director shall—

(1) develop and present to the President an annual budget for the National Foreign Intelligence Program of the United States;

(2) establish the requirements and priorities to govern the collection of national intelligence by elements of the intelligence community;

(3) promote and evaluate the utility of national intelligence to consumers within the Government;

(4) eliminate waste and unnecessary duplication with the intelligence community;

(5) protect intelligence sources and methods from unauthorized disclosure; and

(6) perform such other functions as the President or the National Security Council may direct.

(d) HEAD OF THE CENTRAL INTELLIGENCE AGENCY.—In the Director's capacity as head of the Central Intelligence Agency, the Director shall—

(1) collect intelligence through human sources and by other appropriate means, except that the Agency shall have no police, subpoena, or law enforcement powers or internal security functions;

(2) provide overall direction for the collection of national intelligence through human sources by elements of the intelligence community authorized to undertake such collection and, in coordination with other agencies of the Government which are authorized to undertake such collection, ensure that the most effective use is made of resources and that the risks to the United States and those involved in such collection are minimized;

(3) correlate and evaluate intelligence related to the national security and providing appropriate dissemination of such intelligence;

(4) perform such additional services as are of common concern to the elements of the intelligence community, which services the Director of Central Intelligence determines can be more efficiently accomplished centrally; and

(5) perform such other functions and duties related to intelligence affecting the national security as the President or the National Security Council may direct.

AUTHORITIES OF THE DIRECTOR OF CENTRAL INTELLIGENCE

SEC. 104. [50 U.S.C. 403–4] (a) ACCESS TO INTELLIGENCE.—To the extent recommended by the National Security Council and approved by the President, the Director of Central Intelligence shall have access to all intelligence related to the national security which is collected by any department, agency, or other entity of the United States.

(b) APPROVAL OF BUDGETS.—The Director of Central Intelligence shall provide guidance to elements of the intelligence community for the preparation of their annual budgets and shall approve such budgets before their incorporation in the National Foreign Intelligence Program.

(c) ROLE OF DCI IN REPROGRAMMING.—No funds made available under the National Foreign Intelligence Program may be reprogrammed by any element of the intelligence community without the prior approval of the Director of Central Intelligence except in accordance with procedures issued by the Director.

(d) TRANSFER OF FUNDS OR PERSONNEL WITHIN THE NATIONAL FOREIGN INTELLIGENCE PROGRAM.—(1) In addition to any other authorities available under law for such purposes, the Director of Central Intelligence, with the approval of the Director of the Office of Management and Budget, may transfer funds appropriated for a program within the National Foreign Intelligence Program to another such program and, in accordance with procedures to be developed by the Director and the heads of affected departments and agencies, may transfer personnel authorized for an element of the intelligence community to another such element for periods up to a year.

(2) A transfer of funds or personnel may be made under this subsection only if—

(A) the funds or personnel are being transferred to an activity that is a higher priority intelligence activity;

(B) the need for funds or personnel for such activity is based on unforeseen requirements;

(C) the transfer does not involve a transfer of funds to the Reserve for Contingencies of the Central Intelligence Agency;

(D) the transfer does not involve a transfer of funds or personnel from the Federal Bureau of Investigation; and

(E) the Secretary or head of the department which contains the affected element or elements of the intelligence community does not object to such transfer.

(3) Funds transferred under this subsection shall remain available for the same period as the appropriations account to which transferred.

(4) Any transfer of funds under this subsection shall be carried out in accordance with existing procedures applicable to reprogramming notifications for the appropriate congressional committees. Any proposed transfer for which notice is given to the appropriate congressional committees shall be accompanied by a report explaining the nature of the proposed transfer and how it satisfies the requirements of this subsection. In addition, the Select Committee on Intelligence of the Senate and the Permanent Select Committee on

Intelligence of the House of Representatives shall be promptly notified of any transfer of funds made pursuant to this subsection in any case in which the transfer would not have otherwise required reprogramming notification under procedures in effect as of the date of the enactment of this section.

(5) The Director shall promptly submit to the Select Committee on Intelligence of the Senate and to the Permanent Select Committee on Intelligence of the House of Representatives and, in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and House of Representatives, a report on any transfer of personnel made pursuant to this subsection. The Director shall include in any such report an explanation of the nature of the transfer and how it satisfies the requirements of this subsection.

(e) COORDINATION WITH FOREIGN GOVERNMENTS.—Under the direction of the National Security Council and in a manner consistent with section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), the Director shall coordinate the relationships between elements of the intelligence community and the intelligence or security services of foreign governments on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.

(f) USE OF PERSONNEL.—The Director shall, in coordination with the heads of departments and agencies with elements in the intelligence community, institute policies and programs within the intelligence community—

(1) to provide for the rotation of personnel between the elements of the intelligence community, where appropriate, and to make such rotated service a factor to be considered for promotion to senior positions; and

(2) to consolidate, wherever possible, personnel, administrative, and security programs to reduce the overall costs of these activities within the intelligence community.

(g) TERMINATION OF EMPLOYMENT OF CIA EMPLOYEES.—Notwithstanding the provisions of any other law, the Director may, in the Director's discretion, terminate the employment of any officer or employee of the Central Intelligence Agency whenever the Director shall deem such termination necessary or advisable in the interests of the United States. Any such termination shall not affect the right of the officer or employee terminated to seek or accept employment in any other department or agency of the Government if declared eligible for such employment by the Office of Personnel Management.

RESPONSIBILITIES OF THE SECRETARY OF DEFENSE PERTAINING TO THE NATIONAL FOREIGN INTELLIGENCE PROGRAM

SEC. 105. [50 U.S.C. 403–5] (a) IN GENERAL.—The Secretary of Defense shall—

(1) ensure that the budgets of the elements of the intelligence community within the Department of Defense are adequate to satisfy the overall intelligence needs of the Department of Defense, including the needs of the chairman of the Joint Chiefs of Staff and the commanders of the unified and specified commands and, wherever such elements are performing governmentwide functions, the needs of other departments and agencies;

(2) ensure appropriate implementation of the policies and resource decisions of the Director of Central Intelligence by elements of the Department of Defense within the National Foreign Intelligence Program;

(3) ensure that the tactical intelligence activities of the Department of Defense complement and are compatible with intelligence activities under the National Foreign Intelligence Program;

(4) ensure that the elements of the intelligence community within the Department of Defense are responsive and timely with respect to satisfying the needs of operational military forces;

(5) eliminate waste and unnecessary duplication among the intelligence activities of the Department of Defense; and

(6) ensure that intelligence activities of the Department of Defense are conducted jointly where appropriate.

(b) RESPONSIBILITY FOR THE PERFORMANCE OF SPECIFIC FUNCTIONS.—Consistent with sections 103 and 104 of this Act, the Secretary of Defense shall ensure—

(1) through the National Security Agency (except as otherwise directed by the President or the National Security Council), the continued operation of an effective unified organization for the conduct of signals intelligence activities and shall ensure that the product is disseminated in a timely manner to authorized recipients;

(2) through a central imagery authority (except as otherwise directed by the President or the National Security Council), with appropriate representation from the intelligence community, the continued operation of an effective unified organization within the Department of Defense for carrying out tasking of imagery collection, for the coordination of imagery processing and exploitation activities, and for ensuring the dissemination of imagery in a timely manner to authorized recipients;

(3) through the National Reconnaissance Office (except as otherwise directed by the President or the National Security Council), the continued operation of an effective unified organization for the research and development, acquisition, and operation of overhead reconnaissance systems necessary to satisfy the requirements of all elements of the intelligence community;

(4) through the Defense Intelligence Agency (except as otherwise directed by the President or the National Security Council), the continued operation of an effective unified system within the Department of Defense for the production of timely, objective military and military-related intelligence, based upon all sources available to the intelligence community, and shall ensure the appropriate dissemination of such intelligence to authorized recipients;

(5) through the Defense Intelligence Agency (except as otherwise directed by the President or the National Security Council), effective management of Department of Defense human intelligence activities, including defense attaches; and

(6) that the military departments maintain sufficient capabilities to collect and produce intelligence to meet—

(A) the requirements of the Director of Central Intelligence;

(B) the requirements of the Secretary of Defense or the Chairman of the Joint Chiefs of Staff;

(C) the requirements of the unified and specified combatant commands and of joint operations; and

(D) the specialized requirements of the military departments for intelligence necessary to support tactical commanders, military planners, the research

and development process; the acquisition of military equipment, and training and doctrine.

(c) USE OF ELEMENTS OF DEPARTMENT OF DEFENSE.—The Secretary of Defense, in carrying out the functions described in this section, may use such elements of the Department of Defense as may be appropriate for the execution of those functions, in addition to, or in lieu of, the elements identified in this section.

APPENDIX B

A BRIEF HISTORY OF U.S. INTELLIGENCE

THE EVOLUTION OF THE U.S. INTELLIGENCE COMMUNITY—AN HISTORICAL OVERVIEW

The function of intelligence as an activity of the U.S. Government is often regarded as a product of the Cold War. Indeed, much of what is known today as the Intelligence Community was created and developed during the Cold War period. But intelligence has been a function of the Government since the founding of the Republic. While it has had various incarnations over time, intelligence has historically played a key role in providing support to U.S. military forces and in shaping the policies of the United States toward other countries.

THE EARLY YEARS OF THE REPUBLIC

During the Revolutionary War, General George Washington was an avid user of intelligence as well as a consummate practitioner of the intelligence craft. Records show that shortly after taking command of the Continental Army in 1775, Washington paid an unidentified agent to live in Boston and surreptitiously report by use of "secret correspondence" on the movements of British forces. Indeed, Washington recruited and ran a number of agents, set up spy rings, devised secret methods of reporting, analyzed the raw intelligence gathered by his agents, and mounted an extensive campaign to deceive the British armies. Historians cite these activities as having played a major role in the victory

---

Phyllis Provost McNeil, "The Evolution of the U.S. Intelligence Community—An Historical Overview," in *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, Report of the Commission on the Roles and Capabilities of the United States Intelligence Community [The Aspin-Brown Commission]. Washington, D.C.: U.S. Government Printing Office, March 1, 1996.

at Yorktown and in the ability of the Continental Army to evade the British during the winters at Valley Forge.

In a letter to one of his officers written in 1777, Washington wrote that secrecy was key to the success of intelligence activities:

> The necessity of procuring good intelligence is apparent and need not be further urged—All that remains for me to add is, that you keep the whole matter as secret as possible. For upon Secrecy, success depends in most Enterprises of the kind, & for want of it, they are generally defeated, however, well planned. . . . [letter to Colonel Elias Dayton, 26 July 1777]

Washington was not the only one to recognize the importance of intelligence to the colonials' cause. In November of 1775, the Continental Congress created the Committee of Secret Correspondence to gather foreign intelligence from people in England, Ireland, and elsewhere on the European continent to help in the prosecution of the war.

Washington's keen interest in intelligence carried over to his presidency. In the first State of the Union address in January 1790, Washington asked the Congress for funds to finance intelligence operations. In July of that year the Congress responded by establishing the Contingent Fund of Foreign Intercourse (also known as the Secret Service Fund) and authorizing $40,000 for this purpose. Within three years, the fund had grown to $1 million, about 12 percent of the Government's budget at the time. While the Congress required the President to certify the amounts spent, it also allowed him to conceal the purposes and recipients of the funds. (In 1846, this latter provision was challenged by the House of Representatives, but President Polk, citing national security grounds of protection of sources, refused to turn over more specific information on the use of the Fund to the Congress.) Judging by the paucity of the historical record, interest in intelligence as a tool of the Executive appears to have waned in succeeding Administrations, although occasional lapses in performance sometimes produced controversy. During the War of 1812, for example, military intelligence failed to discover that British troops were advancing on Washington until they were 16 miles from the Capital. The Secretary of War had refused to believe that the British would invade Washington, and military intelligence reported from this perspective.

Intelligence regained prominence during the Civil War. Both the Union and Confederate leadership valued intelligence information, established their own spy networks, and often railed at the press for providing intelligence to the other side. The Confederate forces established the Signal and Secret Service Bureau with the primary charter of obtaining northern newspapers. On the Union side, the Departments of the Navy, State, and War each maintained an intelligence service. Union code-breakers decoded Confederate messages and learned that the plates for Confederate currency were being manufactured in New York. In June of 1861, the first electronic transmission of information was sent from an aerial reconnaissance platform—in this case, a balloon—directly to President Lincoln on the ground. Two months later, Union forces established a Balloon Corps. Although disbanded after two years, it succeeded in detecting a large concentration of Confederate troops preparing to attack at Fair Oaks, Virginia.

In 1863, the first professional intelligence organization was established by the Union forces, the Bureau of Military Intelligence. Headed by the Commander of the Army of the Potomac, General Joseph Hooker, the Bureau prepared evaluations of the Confederate Army's strength and activities based on the sources that included infiltrations of the Confederacy's War and Navy Departments. It was considered the best run intelligence

operation of the Civil War. Yet, Hooker's ineffective use of intelligence (reportedly he was inundated with information) was largely responsible for the Confederate victory at Chancellorsville. Similarly, it has been suggested that Lee's defeat at Gettysburg was partially attributable to his lack of intelligence on the strength and deployment of Union forces.

The Bureau of Military Intelligence was disestablished at the end of the war. A byproduct of its dissolution was the Secret Service, established in 1865 to combat counterfeiting.

A PEACETIME ROLE FOR INTELLIGENCE

Prior to the 1880s, intelligence activities were devoted almost exclusively to support of military operations, either to support deployed forces or to obtain information on the views or participation of other countries in a particular conflict. In March 1882, however, the first permanent intelligence organization—the Office of Naval Intelligence—was created within the Department of t he Navy to collect intelligence on foreign navies in peace-time and in war. Three years later, a similar organization—the Military Intelligence Division—was created within the Army to collect foreign and domestic military data for the War Department and the Army.

The Administration of Theodore Roosevelt saw perhaps the most active use of intelligence for foreign policy purposes by any President until that time. Historians note that Roosevelt used intelligence operatives to incite a revolution in Panama to justify annexing the Panama Canal. In 1907, the President also relied on intelligence that showed the military build-up of the Japanese as justification to launch the worldwide cruise of the "Great White Fleet" as a display of U.S. naval force.

For the most part, however, the early part of the twentieth century was marked no by an expanded use of intelligence for foreign policy purposes, but by an expansion of domestic intelligence capabilities. The Justice Department's Bureau of Investigation (the forerunner of the FBI) was established in 1908 out of concern that Secret Service agents were spying on members of Congress. By 1916, the Bureau had grown from 34 agents focusing primarily on banking issues to 300 agents with an expanded charter that included internal security, Mexican border smuggling activities, neutrality violations in the Mexican revolution, and Central American unrest. After war broke out in Europe, but before the United States joined the Allied cause, the Bureau turned its attention to activities of German and British nationals within our borders.

WORLD WAR I

At the time the United States entered the war, it lacked a coordinated intelligence effort. As a champion of open diplomacy, President Woodrow Wilson had disdained the use of spies and was generally suspicious of intelligence. His views on the subject appeared to change, however, as a result of a close association developed with the British intelligence chief in Washington.

In fact, British intelligence played a major role in bringing the United States into World War I. Public revelations of German intelligence attempts to prevent U.S. industry and the financial sector from assisting Great Britain greatly angered the American public. Subsequently, British intelligence presented Wilson with the decryption of German diplomatic and naval traffic showing a German effort to entice the Mexican government into joining Germany against the United States in return for Texas, Arizona, and New Mexico

if Germany won the war. Later declassified and disclosed to the public, this intercepted communication, known as the "Zimmerman Telegram," infuriated Wilson and added support to his address before a joint session of Congress in 1917 urging that the U.S. declare war on Germany.

In June of 1917, the first U.S. signals intelligence agency was formed within the Army. Known as "MI-8," the agency was charged with decoding military communications and providing codes for use by the U.S. military. In 1919, at the end of the war, the agency was transferred to the State Department. Known as the "Black Chamber," it focused on diplomatic rather than military communications. In 1921, the Black Chamber celebrated perhaps its most significant success by decrypting certain Japanese diplomatic traffic. The intelligence gained from this feat was used to support U.S. negotiators at a Washington conference on naval disarmament. Yet, despite such successes, President Hoover decided that the State Department's interception of diplomatic cables and correspondence could not be tolerated. Apparently agreeing with the alleged, yet oft-quoted statement of his Secretary of State, Henry Stimson, that "Gentlemen do not read each other's mail," Hoover returned the agency to a military orientation under the Army Signal Corps.

Other intelligence entities remained in existence after the end of WWI but saw their resources cut substantially. An exception to this general trend was the Justice Department's Bureau of Investigation, which saw a marked expansion of its mission and workforce. In 1924, J. Edgar Hoover was named director of the Bureau [renamed the Federal Bureau of Investigation (FBI) in 1935]. The FBI's charter was broadened particularly in the years leading to World War II, when concerns for U.S. internal security were mounting in the face of German aggression in Europe. The FBI was made responsible for investigating espionage, counterespionage, sabotage, and violations of the neutrality laws. It was also during this period that the first effort was made to coordinate the activities of the various intelligence elements of the Government. An Interdepartmental Intelligence Coordinating Committee was created for this purpose, but because the Committee lacked a permanent chair and participating agencies were reluctant to share information, it had limited impact.

WORLD WAR II AND ITS AFTERMATH

The years immediately before the United States entered World War II saw American interest in developments in Europe and the Pacific intensify dramatically, prompting both formal and informal efforts to gather and analyze information. President Franklin Roosevelt relied heavily on American and British friends traveling abroad to provide him with intelligence on the intentions of other leaders. One such friend was William J. Donovan, an aficionado of intelligence and a veteran of World War I, whom Roosevelt sent to Europe in 1940 to gather information on Italian Dictator Mussolini, among other matters. Upon his return, Donovan lobbied hard for the creation of a centralized, civilian intelligence apparatus to complement that of the military.

In July 1941, in response to Donovan's urging, Roosevelt appointed Donovan as Coordinator of Information (COI) to form a non-military intelligence organization. The Coordinator of Information was to "collect and analyze all information and data which may bear upon the national security" for the President and those he designated. The Coordinator was given the authority, "with the approval of the President," to request data from other agencies and departments, but was specifically admonished not to interfere with

the duties and responsibilities of the President's military and naval advisers. FBI Director J. Edgar Hoover, fearing a loss of authority to the new Coordinator, secured the President's commitment that the Bureau's primacy in South America would not change.

Borrowing heavily from the British intelligence model, Donovan created a special staff to pull together and analyze all national security information and empaneled an eight-member review board, drawn from academia, to review analysis and test its conclusions. In concert with the Librarian of Congress, COI Donovan organized the Division of Special Information at the Library, to work with Donovan's analytical staff and to coordinate scholarship within the Library and in academia. In theory, the Division was to provide unclassified information to Donovan's staff, who would combine it with classified information to produce an analysis that would be reviewed by the special board before presentation to the President. Although in practice the process did not operate precisely as planned, the concept of centralized analysis was established.

The surprise attack on Pearl Harbor by the Japanese on December 7, 1941, brought America into the war and revealed a significant failure on the part of the U.S. intelligence apparatus. As subsequent investigations found, intelligence had been handled in a casual, uncoordinated manner, and there had been insufficient attention to certain collection requirements. The lack of coordination among agencies, principally the Army and the Navy, resulted in a failure to provide timely decisionmakers. Moreover, intelligence analysts had grossly underestimated Japanese capabilities and intentions, revealing a tendency to misunderstand Japanese actions by looking at them with American cultural biases. After the war, the resolve of America's leaders "never again" to permit another Pearl Harbor largely prompted the establishment of a centralized intelligence structure.

America's entrance into World War II created an immediate need for intelligence to support the warfighter. While the Army and the Navy maintained their own intelligence capabilities, none were prepared to provide the kind of support needed.[1] To bolster this effort, the Office of Strategic Services (OSS) was created in June 1942, under the recently established Joint Chiefs of Staff to succeed the Coordinator of Information. William Donovan remained in charge of the reorganized unit. In addition to assuming the analytical role of its predecessor, the OSS was chartered to carry out clandestine operations against the Axis powers on a worldwide scale. It was not, however, readily accepted by the Joint Chiefs of Staff (JCS), who remained skeptical of the value of OSS activities, and the new unit faced strong competition from the FBI and the Army's intelligence organization.

Usually glamorized as the dashing operations arm of the U.S. Army (with its well-known espionage exploits with the Resistance in Europe), the OSS' contribution to intelligence production has gone largely unnoticed. It was, however, one of the seven major intelligence producers and was an important training ground for a generation of intelligence analysts, as well as operatives. Decidedly different than the British system, the OSS established the tradition of putting analysts and operatives in the same organization. The difficulties, however, that the OSS had in establishing itself within the JCS structure reaffirmed Donovan's belief that the peacetime successor to the OSS should be a civilian organization directly responsible to the President. In 1944, Donovan started campaigning for this model.

In the meantime, substantial intelligence capabilities were created in the military services to support the war effort. Army intelligence operations were supervised by the Military Intelligence Division of the Army General Staff. Its operating arm, the Military Intelligence Service (MIS), was created in 1942 and carried out collection activities around

the world, including agent operations, signals interception, and photo reconnaissance. MIS also provided intelligence analysis to U.S. and allied commands. At the same time, intelligence elements were assigned directly to operating forces in the field. These intelligence units collected and analyzed tactical signals intelligence, interpreted photos, and performed ground reconnaissance missions. Aerial reconnaissance missions were run by the Army Air Corps. To provide counterintelligence support, including the debriefing of prisoners and defectors, the Army Counterintelligence Corps was established in 1942 with both domestic and overseas missions.

Army signals intelligence analysts succeeded in breaking and exploiting the code systems used by the Imperial Japanese Army, producing intelligence which many believe shortened the war in the Pacific. In England, after the U.S. joined the war, Army teams participated in the work begun by the Polish and continued by the British to decode German military communications encrypted with the Enigma cipher machines. The intelligence produced by this effort, codenamed "ULTRA," gave the Allies unparalleled insight into the workings of the German military and shortened the war in Europe.

Within three days of the devastating and embarrassing attack on Pearl Harbor, the Navy's Combat Intelligence Unit at Pearl Harbor was busy trying to crack the Japanese Fleet Code, JN25. By April 1942, enough information was known to allow the American Pacific Fleet to deal the first blow without visual sighting of the Japanese Fleet at the Battle of Coral Sea. By May 1942, Navy cryptanalysts succeeded in cracking the Japanese code. This significant naval intelligence capability, on par with the British and Polish decryption of the German code, allowed the Americans to defeat the Japanese at the Battle of Midway and to countermeasure the Japanese during the rest of the war in the Pacific.

Also in the Pacific theater, an Allied Translator and Interpreter Section, composed of 2,000 American Nisei soldiers, interrogated Japanese prisoners and exploited captured documents. Since the OSS did not operate in the South Pacific Theater, special human source intelligence capabilities were established, using Australian and Philippine guerilla forces as well as a special Army long-distance reconnaissance team known as the Alamo Scouts.

Similarly, the Marine Corps developed and deployed the Navajo Code Talker Program in May 1942. By 1945, operating in both theaters of the War, 400 Native American Navajo members of the Corps were encoding, transmitting, and decoding English messages in the complex language of the Navajo Indians. The Code Talkers have been credited with playing a significant role in the Marine Corps victory on Iwo Jima. So successful was this method of encryption and communication that it was employed in the Korean and Vietnam conflicts.

Toward the end of the war, the Administration was left to decide what to do with these intelligence capabilities. A vigorous and heated debate ensued between those who favored the Donovan idea of an independent, civilian intelligence organization reporting directly to the President and those who favored retention and control of intelligence by the military. The State Department, among others, weighed in heavily against the Donovan approach.

In September 1945, while the debate continued, President Truman, acting on a recommendation from his Budget Director, abolished the OSS by Executive Order and divided its functions between the War and State Departments. State received the research and analysis function, combining it with the existing analytical office to form the Interim Research and Intelligence Service (IRIS). The War Department formed the Strategic Services Unit (SSU) out of the clandestine side of the OSS. President Truman had

unrealized hopes that the State Department would take over the coordination of intelligence for the Government.

At about the time the OSS was being disbanded, a study commissioned by Navy Secretary James Forrestal and chaired by private businessman Ferdinand Eberstadt was published. While the report dealt principally with the issue of military unification, it also recommended coordination of the intelligence function through the establishment of a National Security Council (NSC) and a Central Intelligence Agency (CIA). The NSC would coordinate the civilian and military national security policy for the President. The CIA, under the auspices of the NSC, would serve "to coordinate national security intelligence." While the military generally supported the recommendation calling for centralized coordination of "national security" intelligence, it was unwilling to give up its own collection programs and analytical capabilities.

The Central Intelligence Group

While the recommendations of the Eberstadt study were to influence significantly the content of what eventually became the National Security Act of 1947, they were not immediately implemented. However, President Truman decided to settle the question of whether there should be a centralized civilian intelligence organization.

Reflecting his dissatisfaction with what he perceived to be the haphazard nature of intelligence collection, his desire to have on authoritative source for intelligence advice, and, above all, his desire to avoid another Pearl Harbor, President Truman issued an executive directive on 22 January 1946 establishing a National Intelligence Authority, a Central Intelligence Group (CIG) "under the direction of a Director of Central Intelligence" (DCI), and an Intelligence Advisory Board. The latter body comprised civilian and military heads of intelligence agencies who were to advise to DCI. The National Intelligence Authority, comprising the Secretaries of War, State, Navy, and the President's personal representative, was charged with planning, developing, and coordinating the intelligence effort. Finally, the CIG (a small interdepartmental group—not an independent agency) was responsible for coordinating, planning, evaluating, and disseminating intelligence and overtly collected information. Funding and staffing of the CIG were provided by other departments and agencies which retained control over their own intelligence efforts.

The first DCI, Rear Admiral Sidney Souers (who wrote the intelligence section of the Eberstadt study), reluctantly accepted the appointment and stayed in the position only six months. Under his tenure, the CIG played a limited analytical role due to Souers' reluctance to challenge the analytical product of the State Department's IRIS. But the IRIS was soon decimated by congressional budget cutting, and most of its positions were dispersed throughout the Department and to other agencies. In all, 600 positions were transferred from the IRIS to the National Intelligence Authority, the CIG, and the military services. This left the Department with a skeleton analytic group, thus limiting its mission to providing intelligence support only to the policymakers within the Department of State.[2]

The second DCI, Lieutenant General Hoyt Vandenberg, proved more aggressive than his predecessor, gaining authority for the CIG to hire personnel and acquire its own administrative support, as well as expanding clandestine collection, research and analysis, and the overall size of the organization. At the behest of the President, the first national estimate, on Soviet intentions and capabilities, was produced in 1946 during Vandenberg's tenure.

At the time Vandenberg became DCI, in June of 1946, legislation was being drafted in the Congress and in concert with the Truman Administration to provide for the unification of the military establishment under a Secretary of Defense. Inasmuch as the CIG would need an annual appropriation to continue in existence, Vandenberg saw an opportunity to incorporate legislative language creating an independent central intelligence agency with several features modeled on the existing charter of the CIG. Within a month of assuming the duties of DCI, Vandenberg submitted a proposal describing this new entity, with the support of the Truman Administration, which consisted basically of the pertinent language from the 1946 presidential directive and language that had been previously published in the Federal Register.

The National Security Act of 1947

In the ensuing congressional debate on the Vandenberg proposal, several issues emerged about the role of the DCI.

One was whether the DCI should be a civilian or military office. Some argued that if the DCI were an active duty military officer, he would be subject to the control of his parent service. On the other hand, the military was recognized as the principal consumer of intelligence and controlled most of the resources devoted to it. The legislation ultimately provided that the President could appoint either a civilian or a military officer as the DCI, but if a military officer were appointed, he would be removed from the control of his parent service.

Another issue was whether the DCI should be a member of the National Security Council that was being established by the bill as the White House focal point for national security matters. Navy Secretary James Forrestal argued strongly against this proposal saying that the Council would be too large to accomplish its business and that the new DCI would have ready access without formal membership. His argument was persuasive and the DCI's proposed membership on the NSC was dropped.

A third issue was the relationship of the DCI to other agencies, in particular, the FBI. The draft proposal provided that the new Central Intelligence Agency would serve as the focal point within the Government where intelligence would be gathered and evaluated. As such, the CIA would necessarily require access to information collected by other agencies. The military agreed to this coordinating role for the CIA so long as the military was able to maintain its own collection and analytical capabilities to support military operations. The FBI, however, insisted on limiting the CIA's access to FBI files only if written notice was given first and only if access was "essential to the national security."

On July 27, 1947, President Truman signed into law the National Security Act of 1947, creating a postwar national security framework. A National Security Council was created to coordinate national security policy. The Act created the position of Secretary of Defense and unified the separate military departments (the Army, the Navy, and the newly-created Air Force) under this position. The Act also established the Joint Chiefs of Staff to serve as the principal military advisers to the President and the Secretary of Defense. Finally, a Central Intelligence Agency was established with the Director of Central Intelligence as its head. At the time of its creation, the CIA was the only agency charged with a "national" intelligence mission.

The statutory language regarding the authorities and functions of the new Central Intelligence Agency was left intentionally vague. In part this reflected the bureaucratic

sensitivities involved in specifying in the law the DCI's roles and missions in regard to other agencies, and, in part the desire to avoid wording that other governments might find offensive. Thus, there was no mention of "espionage" or "spying" in the statute, nor was there any wording to suggest that covert actions (i.e., secret operations to influence political conditions in other countries) were part of the new agency's charter. Rather, the CIA was authorized to perform "services of common concern" to other intelligence agencies as may be determined by the National Security Council and to perform "such other functions and duties related to intelligence affecting the national security as the National Security Council may from time-to-time direct." (The NSC did, in fact, issue directives in 1947 and 1948, providing specific authority for CIA's operational and analytical functions.)

The 1947 Act also included an express prohibition on the CIA's having any "police, subpoena, law-enforcement powers, or internal security functions," reflecting the congressional and public desire to ensure that they were not creating a U.S. "Gestapo" and to preserve the FBI's primacy in domestic matters. The law also made the DCI responsible for "protecting intelligence sources and methods from unauthorized disclosure."

The Early Years of the CIA

The early years of the CIA appear to have been difficult ones as the Agency attempted to establish itself within the Government, amid growing concern about Communist gains in Eastern Europe and Soviet expansionism.

Rear Admiral Roscoe Hillenkoetter was DCI at the time the CIA was created. He organized the Agency into two principal divisions: one dealing with intelligence operations and the other with analysis. The analytical arm, in response to policymaker interest, prepared and disseminated short-term intelligence pieces. DCI Hillenkoetter found it difficult, however, to force other agencies to participate in the development of longer papers despite the language of the 1947 Act. The emphasis on producing short-term pieces, on the other hand, was often seen as intruding on the role of other producers such as the State Department, the military departments, and the FBI. There was also conflict on the operational side. The Government considered initiating psychological warfare operations overseas to counter Soviet expansionism, but the NSC preferred that the State Department, rather than the CIA, be responsible for them. It was only when the Secretary of State vigorously objected to this role for the Department that it was assigned to the CIA.

In January 1948, less than a year after the CIA was created, the National Security Council, exercising its overnight role under its Executive Secretary Sidney Souers,[3] asked three private citizens to examine comprehensively CIA's "structure, administration, activities, and interagency relations." Allen Dulles, William Jackson and Matthias Correa, three New York lawyers with experience in intelligence, submitted their highly critical report in January 1949. Although the NSC found the criticism of DCI Hillenkoetter and the CIA "too sweeping," it nevertheless accepted the report's basic findings: CIA was not coordinating intelligence activities in the Government; the correlation and evaluation functions were not well organized, and other members of the fledgling Intelligence Community were not fully included in the estimates process; and the DCI lacked sufficient day-to-day contact with the work of CIA. The Dulles-Jackson-Correa report called upon the DCI to exert "forthright leadership," and to actively use existing coordination bodies, such as the Intelligence Advisory Committee (IAC) comprising the leaders of the military and civilian intelligence agencies. For example, the report urged that the final coordination

of intelligence estimates be done through IAC, to establish estimates as "the most authoritative statement[s] available to policymakers."

The Dulles-Jackson-Correa report also made the point that coordination and planning could only be effective with a strong DCI and CIA. It therefore recommended that the DCI reorganize his office to include on his immediate staff the heads of CIA's main components. The report also stated that the CIA would benefit from civilian leadership and recommended that if another military DCI was appointed, he should resign his military commission "to free him from all service ties and from rotations that would preclude the continuity needed for good intelligence work."[4]

Also during 1948, the Congress established "The Commission on Organization of the Executive Branch of the Government." Chaired by former President Herbert Hoover, the Commission established a sub-group to look at national security organizations, including CIA. This group, headed by New York businessman Ferdinand Eberstadt,[5] concluded that the basic organizational arrangements for national security were sound, but there were problems in carrying out the function. The CIA was specifically criticized for not being properly organized to assimilate all information concerning scientific developments abroad, to estimate the significance of these developments, and to give direction to collectors. Concern was also expressed that the CIA was not being given access to all available information within the Government. The fear that other countries might develop nuclear weapons led the Eberstadt group, with some urgency, to state:

> Failure properly to appraise the extent of scientific developments in enemy countries may have more immediate and catastrophic consequences than failure in any other field of intelligence.

In its November 1948 report, the Hoover Commission called for "vigorous efforts" to improve CIA's internal structure and the quality of its product, especially in scientific and medical intelligence. A senior-level "evaluation board or section" within CIA was proposed to work solely on intelligence evaluations. Finally, the Commission urged positive efforts to foster "relations of mutual confidence" between CIA and its consumers.[6]

Lieutenant General Walter Bedell Smith, who succeeded Hillenkoetter as DCI soon after the outbreak of the Korean War, took the initial steps to implement the recommendations of the Hoover and the Dulles-Jackson-Correa reports. Among his first steps was to recruit Allen Dulles, an OSS veteran, as Deputy Director for Plans, and to establish a Board of National Estimates chaired by William Langer of Harvard University.

In 1949, Congress enacted additional legislation for the CIA providing its Director with certain administrative authorities necessary for the conduct of clandestine intelligence activities that were not available to government agencies generally. In particular, the new law permitted the DCI to expend appropriated funds for procuring goods and services to carry out the Agency's functions without having to comply with the cumbersome procurement rules applicable to other government agencies. It also permitted the Agency to expend appropriated funds based solely on a voucher signed by the DCI.

1950s AND 1960s: THE DEVELOPMENT OF THE INTELLIGENCE COMMUNITY

The decades of the 1950s and 1960s saw an expansion and an intensification of the Cold War as well as an expansion in the size and responsibilities of U.S. intelligence agencies to cope with its challenges.

The 1950s

Acting on the recommendations of a commission of senior officials headed by George Brownell, President Truman, by classified memorandum, established the National Security Agency (NSA) in October 1952 in recognition of the need for a single entity to be responsible for the signals intelligence mission of the United States. Placed within the Department of Defense, NSA assumed the responsibilities of the former Armed Forces Security Agency as well as the signals intelligence responsibilities of the CIA and other military elements. In 1958, the National Security Council issued directives that detailed NSA's mission and authority under the Secretary of Defense.

CIA meanwhile made important strides. Its analytical efforts during the Korean War established the Agency as a key player in the defense and foreign policy areas. On the operational side, the National Security Council reissued its 1948 directive on covert action to achieve peacetime foreign policy objectives in 1955, reemphasizing that implementation responsibility was with the CIA. In 1954, President Eisenhower approved the concept of a high-flying reconnaissance aircraft to fly above the Soviet air defense systems. Due largely to CIA's special procurement authorities and ability to carry out the mission in secret, the President established the effort as a joint CIA-Air Force program. The ability of the program to develop and field the U-2 (by 1955) earlier than planned and below the original cost estimate was a clear success for the participants. Before the end of the decade photos provided by the U-2 figured prominently in defense planning.

In 1954, Congress once again sought to examine the organization and efficiency of the Executive Branch and revived "The Commission on Organization of the Executive Branch of the Government." With former President Hoover again at the helm, the "Second Hoover Commission" formed a sub-group headed by General Mark Clark to study the agencies of the Intelligence Community.[7]

The Clark task force recommended that the CIA be reorganized internally to focus better on its primary missions, and that the DCI appoint a "Chief of Staff" or executive officer to run the day-to-day operations.[8] It also called for a permanent "watchdog" commission to oversee the CIA, comprising members of the House and Senate and distinguished private citizens appointed by the President.[9] A year later, in 1956, President Eisenhower established the Presidential Board of Consultants on Foreign Intelligence Activities (later renamed the President's Foreign Intelligence Advisory Board by President Kennedy). Shortly after it was formed, the Board issued a critical review of the DCI's management of the Intelligence Community. Later, in 1957, on the Board's recommendation, President Eisenhower established the United States Intelligence Board as the single forum for all intelligence chiefs to provide advice to the DCI on intelligence activities.

In 1957, spurred by the Soviet launch of Sputnik, the CIA and the Air Force began planning for the first photo reconnaissance satellite. Publicly referred to as "the Discoverer Weather System" and recently declassified as "CORONA," the system was successfully operational by 1962.

The 1960s

The decade of the 1960s was marked by significant technological advances, further expansion of the Intelligence Community, and the first tentative efforts of a DCI to exert control over it. But, as far as the public was concerned, it started with the notable failure of

the CIA at the Bay of Pigs. An invasion of Cuban expatriates, trained by the CIA, launched an invasion of Cuba in the spring of 1961 with the intent of ousting the Castro regime. Without U.S. military assistance, the invasion crumbled. The reputation of the Agency suffered significantly.

In August of the same year, Secretary of Defense McNamara created the Defense Intelligence Agency (DIA) to consolidate and to coordinate the production of intelligence analysis by each of the military services and to serve as the principal source of intelligence support to the Secretary and his staff, as well as to the Joint Chiefs of Staff and the unified commands. DIA opened a new production center in 1963, but the military departments continued to maintain their own analytical capabilities. In 1965, DIA was given responsibility for administering the newly-created Defense Attache system, consisting of uniformed military personnel serving in embassies and collecting, by overt means, information useful to the military.

In the meantime, there were substantial advances in U.S. technical collection capabilities. Photographs taken by the U-2 were a large factor in the successful resolution of the Cuban missile crisis in 1962. The first photo reconnaissance satellite was launched the same year. The first high altitude, high speed reconnaissance aircraft, the SR-71, was built and tested by the CIA a short while later. While these technical collection efforts had been ongoing for several years in both CIA and the Air Force, they were formally consolidated, pursuant to a national security directive, in 1961 within the National Reconnaissance Office (NRO).

While the fact of its existence remained classified, the NRO was designated a separate operating agency of the Department of Defense, reporting to the Secretary of Defense albeit with the DCI retaining a role in selecting key personnel as well as substantial control over the budget, requirements, and priorities of the organization. Using the special procurement authorities of the DCI, the NRO was able expeditiously to procure and to operate satellite collection systems for the Intelligence Community.

In addition to the NSA, DIA, and NRO, each of the military services maintained substantial intelligence organizations, both at the departmental level and at the tactical level. These organizations typically collected information and provided analysis regarding the weapons systems, tactics, and capabilities of foreign counterpart forces. This information and analysis were used to support the weapons acquisition process in each service, to support force development and contingency planning, and were incorporated into training programs.

The growth of intelligence efforts within the Department of Defense served to accentuate the relative lack of the DCI's role over the rest of the Community. In July 1961, the President's Foreign Intelligence Advisory Board proposed to the President that the DCI be separated from the CIA and head-up an Office of Coordination in the White House. President Kennedy did not endorse the recommendation but in January 1962 issued a letter to his new DCI John McCone stating:

> As head of the Central Intelligence Agency, while you will continue to have overall responsibility for the Agency, I shall expect you to delegate to your principal deputy, as you may deem necessary, so much of the detailed operation of the Agency as may be required to permit you to carry out your primary task as Director of Central Intelligence.

In 1963, DCI McCone established a National Intelligence Programs Evaluation Staff to review and evaluate Community programs and cost-effectiveness. Later in the decade,

DCI Helms set up a National Intelligence Resources Board to review all community programs and budgets, and to referee community disputes.[10]

But the burgeoning U.S. military involvement in the Vietnam War, the efforts to block Communist expansion in Laos and to deal with conflicts in the Middle East (notable the Arab-Israeli Six-Day War of 1967), effectively precluded serious efforts by the DCIs to assert greater control over the Intelligence Community.

THE 1970s: THE DECADE OF TURMOIL AND REFORM

The decade of the 1970s began with serious efforts to institute DCI control over the Intelligence Community, but they were eventually undermined by a series of sensational disclosures in the media, followed by unprecedented investigations of the Intelligence Community within the Executive Branch and by the Congress. During the latter half of the decade, new reforms were adopted and new oversight mechanisms put into place. While the intelligence functions of the Government continued, Congress began to take a much more active role in determining their cost and overseeing their execution.

In December 1970, President Nixon directed Deputy Director of the Office of Management and Budget James Schlesinger to recommend how the organizational structure of the Intelligence Community should be changed to bring about greater efficiency and effectiveness. The Schlesinger report, completed in March 1971, found, among other things, that intelligence functions were fragmented and disorganized; collection activities were unnecessarily competitive and redundant; intelligence suffered from unplanned and unguided growth; intelligence activities were too costly; and, because analytical products were provided on such a broad range of topics, they often suffered in quality. The report called for basic reform of the management structure with a strong DCI who could bring intelligence costs under control and improve analytic quality and responsiveness. Among other things, the study recommended that the DCI put together a consolidated budget for the Intelligence Community and oversee its execution.

Following-up on the recommendations in November 1971, President Nixon issued a directive calling for improvement in the intelligence product and for more efficient use of resources. The DCI was made responsible for "planning, reviewing, and evaluating all intelligence programs and activities and in the production of national intelligence." The Nixon directive reconstituted the United States Intelligence Board to assist the DCI, and set up the Intelligence Committee[11] of the NSC to coordinate and to review intelligence activities. It also established an Intelligence Resources Advisory Committee, comprising representatives from the State and Defense Departments and OMB, to advise the DCI on the consolidated intelligence budget. In March 1972, DCI Helms created a special "Intelligence Community Staff" to assist him in the daily execution of his Community responsibilities.

None of these changes had a substantial impact at the time, however, because the Government became largely preoccupied with the Watergate affair in 1973 and 1974. There was only tangential involvement by the CIA in Watergate primarily through the activities of former employees, and in the preparation of a psychological profile of Daniel Ellsberg.[12] The press, however, motivated to some extent by the distrust generated by Watergate, increasingly began to report critically on intelligence activities. Press articles covered allegations of collection efforts undertaken against U.S. citizens during the Vietnam era, attempts to assassinate foreign leaders or destabilize communist regimes, and efforts to raise the remains of a Soviet submarine off the floor of the Pacific.

In December 1974, in reaction to reports of CIA's support to the non-Communist resistance forces in Angola, Congress passed an amendment to the Foreign Assistance Act, known as the "Hughes-Ryan amendment," which for the first time required that the President report any covert CIA operations in a foreign country (other than for intelligence collection) to the relevant congressional committees (which, at that time, included the armed services committees, foreign relations committees, and appropriations committees in each house of Congress).

The various media revelations also led to official investigations in both the Executive branch and the Congress:

A. The Rockefeller Commission

The Commission on CIA Activities Within the United States, chaired by Vice President Rockefeller, was created by President Ford on 4 January 1975, to determine whether CIA employees had engaged in illegal activities in the United States. The inquiry was later expanded to include the CIA's foreign intelligence charter and to make suggestions for operational guidelines. In June 1975, the Commission issued its report which, among other things, confirmed the existence of a CIA domestic mail opening operation; found that in the late 1960s and early 1970s the Agency had kept files on 300,000 U.S. citizens and organizations relating to domestic dissident activities; found that President Nixon tried to use CIA records for political ends; and concluded that the CIA had no involvement in President Kennedy's assassination. The Commission also found "that the great majority of the CIA's domestic activities comply with its statutory authority." In looking to the future, the Commission called for a joint congressional oversight committee and a stronger executive oversight mechanism; consideration by the Congress to disclose "to some extent" CIA's budget; and appointment of two confirmed deputy directors, one to manage the CIA and one to advise the DCI on military matters. The Commission further recommended that the DCI serve no more than 10 years.

B. The Church Committee

Twenty-three days after the Rockefeller Commission was empaneled, the Senate announced its own investigatory body, the Committee to Study Government Operations with Respect to Intelligence Activities (also known as the Church Committee after its Chairman). Handling one of the largest investigations ever undertaken by the Senate, the Church Committee was charged with looking at CIA domestic activities; covert activity abroad, including alleged assassinations of foreign leaders; alleged abuses by the Internal Revenue Service and the FBI; alleged domestic spying by the military; and the alleged interceptions of the conversations of U.S. citizens by the National Security Agency. The Committee's inquiry lasted for almost a year; resulting in a six-volume report, released in April 1976. The Committee recommended, among other things, that the President consider separating the DCI from the CIA; that the authorities of the DCI over elements of the Intelligence Community be enhanced; that statutory charters be established for the CIA, DIA, and NSA; that the National Foreign Intelligence Budget be published; and that clandestine support to repressive regimes that disregarded human rights be prohibited by law. The Committee lauded several reforms (including a ban on assassination) already implemented by President Ford.

C. The Pike Committee

The House counterpart to the Church Committee was the Select Committee on Intelligence to Investigate Allegations of Illegal or Improper Activities of Federal Intelligence Agencies. Impanelled in February 1975, the committee was also known by the name of its Chairman, Congressman Otis Pike. The Pike Committee's report was voted down by the House in January 1976, and was never officially issued. Portions, however, were leaked to a New York newspaper, the *Village Voice*.

D. The Murphy Commission

In June 1975, around the time that the Rockefeller Commission was completing its inquiry into intelligence improprieties, another congressional commission, the Commission on the Organization of the Government for the Conduct of Foreign Policy, was culminating a three-year study which included an examination of the organization and performance of the Intelligence Community. Headed by veteran diplomat Robert Murphy,[13] the Commission recommended that the DCI be given greater status in the White House and the Intelligence Community; that the DCI delegate his responsibility for running the CIA to a deputy; that the DCI occupy an office geographically closer to the White House to better enable him to carry out his role as presidential adviser; and that the CIA change its name to the Foreign Intelligence Agency.[14] The Commission also recommended that covert action should be employed only where it is clearly essential to vital U.S. purposes and only after a careful process of high level review. It further urged that the NSC's Committee on Intelligence be actively used as the principal forum to resolve the differing perspectives of intelligence consumers and producers, and "should meet frequently for that purpose."

Reform and Oversight

Even as the Church and Pike Committees were continuing their investigations, the Executive branch undertook extensive efforts to bring about reform.[15]

In the summer of 1975, President Ford ordered the implementation of 20 of the 30 recommendations of the Rockefeller Commission, to include measures to provide improved internal supervision of CIA activities; additional restrictions on CIA's domestic activities; a ban on mail openings; and an end to wiretaps, abuse of tax information, and the testing of drugs on unsuspecting persons. Ford did not agree to public disclosure of the intelligence budget, however, nor did he readily agree to a separate congressional oversight committee.

President Ford issued the first Executive Order on intelligence on 18 February 1976 (E.O. 11905),[16] before either the Church or Pike investigating committees had reported. For the first time, a description of the Intelligence Community and the authorities and responsibilities of the DCI and the heads of other intelligence agencies, were specified in a public presidential document. The order also set up a Committee on Foreign Intelligence as part of the National Security Council, chaired by the DCI and reporting directly to the President, as the focal point for policy and resource allocation on intelligence.[17] A number of restrictions on intelligence agencies were also instituted, including a ban on assassinations as an instrument of U.S. policy. To monitor compliance with the Order, a new Intelligence Oversight Board was established within the Executive Office of the President.

Both congressional investigating committees recommended in their final reports that permanent follow-on committees be created to provide oversight of the intelligence function and to consider further legislative actions as might be necessary.

The Senate acted first in May 1976, creating the Select Committee on Intelligence. The House followed suit a little over a year later, creating the Permanent Select Committee on Intelligence. Both committees were made responsible for authorizing expenditures for intelligence activities (although the Senate was limited to "national" intelligence, whereas the House mandate included both "national" and "tactical" intelligence activities), and for conducting necessary oversight. The resolutions creating both committees recognized that they would be kept "fully and currently informed" of intelligence activities under their purview. Both committees were added to the list of those to receive notice of covert actions under the Hughes-Ryan amendment. The Senate committee also was given responsibility for handling the confirmation proceedings when the DCI and the Deputy DCI were nominated by the President.

While efforts were made in succeeding months to let emotions over intelligence activities subside and to establish more "normal" relationships between the Legislative and Executive branches, the hiatus was relatively short-lived. In 1977, the Senate Committee reexamined the question whether the aggregate intelligence budget should be released publicly. This issue would continue to be debated for the next two decades. The statement of newly-appointed DCI Turner that he had no problem with the release of this figure aroused protests from those who believed disclosure could assist hostile intelligence services in deciphering U.S. intelligence activity.

In August 1977, DCI Turner prompted a more substantial controversy by announcing his intention to reduce the CIA's Directorate of Operations by 800 people. The first reductions occurred on 31 October 1977 (called the "Halloween Massacre" within CIA) when 200 officers were fired. Critics of the DCI charged that he was destroying the CIA's human source collection capability in favor of technical collection programs run by the Department of Defense. (Some in Defense, on the other hand, perceived Turner as attempting to take over those programs.)

On 24 January 1978, President Carter issued a new Executive Order on intelligence which reaffirmed the DCI's Community-wide authority over priorities, tasking, and the budget; contained additional restrictions on collection techniques, participation in domestic activities, and human experimentation; and reiterated the ban on assassinations. Intelligence agencies were specifically required to promulgate procedures to govern the collection of information on U.S. citizens and persons admitted to the U.S. for permanent residence.

Notwithstanding the new presidential order, both congressional committees proceeded to consider bills in 1978 which would have dramatically overhauled the Intelligence Community. Following the suggestions of the Church Committee as well as incorporating various aspects of the Executive branch reforms, the Senate committee developed a comprehensive bill entitled the "National Intelligence Reorganization and Reform Act of 1978." The bill called for the creation of a "Director of National Intelligence" with broader powers than the DCI to serve as head of the Intelligence Community. The Director of National Intelligence would have retained leadership of CIA[18] with the authority to delegate this responsibility to a Deputy or Assistant Director at the President's discretion. The bill also contained a long list of restricted or banned activities, provided specific missions and functions for each element of the Intelligence Community, stipulated

rigorous review and notification procedures for covert action and clandestine collection, and instituted numerous requirements for reporting to Congress.

While the Carter Administration initially supported the attempt to draft "charter" legislation, it ultimately withdrew its support in the face of growing concern that the intelligence function would be hamstrung by having too much detailed regulation in statute. After extended negotiations with the two intelligence agencies, the Administration agreed to a measure limited to establishing the ground rules for congressional oversight. The Intelligence Oversight Act of 1980 provided that the heads of intelligence agencies would keep the oversight committees "fully and currently informed" of their activities including "any significant anticipated intelligence activity." Detailed ground rules were established for reporting covert actions to the Congress, in return for the number of congressional committees receiving notice of covert actions being limited to the two oversight committees.

Congress also passed, with the support of the Carter Administration, the Foreign Intelligence Surveillance Act of 1978, providing for a special court order procedure to authorize electronic surveillance for intelligence purposes, activities that had previously been conducted based upon a claim of constitutional authority of the President.

Finally, in response to continued criticism from the congressional committees over the usefulness of national intelligence estimates, a new mechanism for the development of estimates was established. DCI Colby, in 1973, had established the National Intelligence Officer system in lieu of the Board of Estimates. He had appointed the first six NIOs in an effort to make intelligence more responsive to policymaking. By the end of the decade, DCI Turner formed the NIOs into the National Intelligence Council. Reporting to the DCI, the Council comprised a Chairman and eight National Intelligence Officers, who were considered the senior analysts of the Intelligence Community within their respective areas of expertise. As such, they would supervise the preparation of estimates, ensure quality control, and present the results of their work to policymakers as required.

1980s: A DECADE OF GROWTH AND SCANDAL

The beginning of the decade saw the election of a new President, Ronald Reagan, who had made the revitalization of intelligence part of his campaign. Intelligence budgets were increased, and new personnel were hired. The vast majority of rules and guidelines adopted during the Ford and Carter Administrations remained in place. However, by the middle of the decade, the U.S. experienced a series of spy scandals, and the first serious breach of the oversight arrangements with the Congress. While the organization of the Intelligence Community remained stable during the decade, it was a period of burgeoning growth and activity.

During the 1980 presidential election, intelligence became a targeted campaign issue. The Republican Party platform contained a plank asserting that the Democrats had impaired the efficiency of the Intelligence Community and had underestimated the Soviet's military strength. President Reagan came into office promising to improve intelligence capabilities by upgrading technical systems and strengthening counterintelligence.

To make good on these promises, Reagan appointed William Casey, a veteran of the OSS, as DCI, and announced that the DCI, for the first time, would hold cabinet rank. With this presidential mandate, Casey sought and received higher budgets for intelligence and instituted an unprecedented period of personnel growth across the Intelligence Community.

On 4 December 1981, almost a year into his Administration, President Reagan issued his Executive Order on Intelligence (E.O. 12333). It generally reaffirmed the functions of intelligence agencies (as outlined in the previous order) and continued most of the previous restrictions, but it set a more positive tone than its predecessor, and gave the CIA greater latitude to gather foreign intelligence within the United States and to provide assistance to law enforcement. The Executive Order also provided a new NSC structure for reviewing intelligence activities, including covert actions.[19]

Meanwhile, the congressional intelligence committees demonstrated a willingness to provide legislative authority sought by the Intelligence Community. In 1980, the Classified Information Procedures Act was passed to protect classified information used in criminal trials. In 1982, following the public revelation of the names of certain CIA officers that appeared to result in the murder of one officer, the Congress passed a new law making it a crime to reveal the names of covert intelligence personnel. In October 1984, Congress exempted certain operational files of the CIA from disclosure under the Freedom of Information Act. However, legislative proposals offered in 1984 calling for a fixed term for the DCI and Deputy DCI and requiring that they be career intelligence officers, were not passed.

The 1986 Goldwater-Nichols Act, which reorganized the Department of Defense and shifted authority from the military departments to the Joint Chiefs and theater commands, also had an impact on intelligence. The Defense Intelligence Agency and Defense Mapping Agency were specifically designated as combat support agencies, and the Secretary of Defense, in consultation with the DCI, was directed to establish policies and procedures to assist the National Security Agency in fulfilling its combat support functions. The Act also required that the President submit annually to Congress a report on U.S. national security strategy, including an assessment of the adequacy of the intelligence capability to carry out the strategy.

1985: The Year of the Spy

Beginning in 1985, the Intelligence Community experienced an unprecedented rash of spy cases that led to numerous recommendations for change.

The defection of former CIA officer Edward Lee Howard in the spring of 1985 was followed by the arrests of John A. Walker, Jr. and Jerry A. Whitworth, Navy personnel with access to highly sensitive information; CIA employees, Sharon Scranage and Larry Wu-Tai Chin; former NSA employee, Ronald W. Pelton; FBI agent, Richard Miller; and an employee of Naval intelligence, Jonathan J. Pollard. The Walker-Whitworth, Pelton, and Howard cases dealt especially serious blows to U.S. intelligence. As the year drew to a close, a Marine guard at the U.S. Embassy in Moscow confessed to having passed information to the Soviets and was charged with allowing Soviet personnel to enter the chancery building. It was further disclosed that the U.S. had determined its new chancery in Moscow had been thoroughly bugged during its construction. Coming in close succession, these disclosures shocked the public and the Congress.

Various efforts were taken within the Executive branch to identify and correct shortcomings in counterintelligence and security. The Secretary of Defense commissioned a special inquiry into Defense policy and practice. The Secretary of State commissioned a review of embassy security, including the vulnerability of U.S. diplomatic establishments to electronic penetration. The CIA undertook an internal review of counterintelligence and its procedures for handling defectors.

The congressional intelligence committees also investigated these problems and prepared lengthy reports recommending change. In 1988, the Senate committee asked a group of distinguished private citizens, led by New York businessman Eli Jacobs, to review the progress that had been made in counterintelligence and to provide recommendations for further improvements. Their report was provided in 1989, but did not result in any legislation being enacted at the time. This was due in part to the fall of the Berlin Wall, and dramatic changes taking place in the Soviet Union, which lessened the intensity of focusing on problems with spies.

The Iran-Contra Affair and Its Aftermath

In November 1986, Congress learned that representatives of the Reagan Administration, contrary to the announced policies of the Government, had sold arms to the Government of Iran in return for its assistance in securing the release of U.S. hostages held in Lebanon. Initiated by members of the NSC staff, the operation was accomplished with the assistance of some officers of the CIA and the Defense Department pursuant to a retroactive covert action "finding" signed by President Reagan in January 1986, which had never been reported to the Congress. It was also disclosed that the NSC staff members involved in the sales had overcharged the Iranians for the weapons and had used the proceeds to support the anti-Communist rebels, the "Contras," in Nicaragua at a time when such assistance was prohibited by law. The veracity of public statements made by the President and other senior officials with knowledge of the episode appeared in doubt. CIA and other intelligence agencies were quickly drawn into the controversy, which collectively became known as the Iran-Contra affair.

A special prosecutor was appointed to look into possible criminal activity, and investigations ensued in both the Executive branch and the Congress. In December 1986, the President commissioned a Special Review Board, chaired by former Senator John Tower. Three months later, the Tower Board found that the Iran and Contra operations were conducted outside of regularly established channels and that intelligence oversight requirements had been ignored. The Board also faulted President Reagan's management style. While not recommending organizational changes *per se*, the Board urged that a better set of guidelines be developed for approving and reporting covert action. The Board also recommended that Congress consider merging the two intelligence committees into a single joint committee.

In early 1987, the House and Senate formed separate investigating committees, but later agreed to form a Joint Committee for purposes of interviewing witnesses and holding hearings. After months of intense public hearings, a majority of the Committee issued a lengthy account of its work in the fall of 1987. It recommended, among other things, that a statutory Inspector General be created at the CIA and that the legal requirements for reporting covert actions to the congressional oversight committees be tightened.

Lawrence Walsh, the special prosecutor appointed in January 1987, carried on his investigation of the Iran-Contra affair for almost seven years, and brought criminal prosecutions against the key NSC figures involved, some CIA employees, and a former Secretary of Defense. President Bush later issued pardons to six of those charged.

Legislation creating a statutory Inspector General for the CIA was enacted in 1989. Although the Inspector General reported to the DCI, he could be removed only by the President. Among other things, the law required that the Inspector General submit semi-annual

reports to the congressional intelligence committees, summarizing problems that had been identified and corrective actions taken.

Legislative efforts to tighten the covert action reporting requirements did not succeed for several more years. In 1988, with the election of President George Bush, a former DCI, Congress received assurances that the experience of Iran-Contra would not be repeated and that appropriate consultations would occur on future covert actions. These assurances did not put the matter to rest as far as the committees were concerned, but did serve to dampen congressional fervor to legislate precise time requirements for reporting.

1990–1995: THE END OF THE COLD WAR AND RETRENCHMENT

The three years following the election of President Bush saw profound changes in the world that had enormous impacts on the Intelligence Community. In the fall of 1989, the Berlin Wall came down and Germany began the process of reunification. The Communist regimes of Eastern Europe gave way to democratic rule. In August 1990, Iran invaded Kuwait. Shortly thereafter, the Soviet Union began to break apart with many former Soviet Republics declaring independence. In early 1991, the U.S. together with NATO allies (and the agreement of the Soviet Union) invaded Kuwait to oust the occupying Iraqi forces with a fearsome display of modern weaponry. Later in the year, Communist rule ended in Russia.

Some began to question whether an intelligence capability was needed any longer; others urged significant retrenchment. Leaders within the Intelligence Community began streamlining their agencies and reorienting toward new missions, with a greater focus on transnational threats. Congress pushed them along by proposing a new Intelligence Community structure, and mandating across-the-board reductions in personnel.

The period ended with a shocking new spy case at the CIA and renewed calls for reform.

The Gulf War

The Gulf War of 1991, brief though it was, had profound repercussions for U.S. intelligence. Never had so much information been conveyed so quickly from intelligence systems to warfighters with such devastating effect. The accuracy of U.S. precision guided weapons astounded the world. The war also highlighted the need for the United States to expand its own efforts to link intelligence systems with combat systems and to train military personnel to use these systems effectively. The U.S. recognized that the future of warfare was apt to be battles fought at a distance between opposing forces, placing a premium on the availability of intelligence on the nature and disposition of hostile forces.

Yet the Gulf War also demonstrated problems with intelligence. Initially, the Intelligence Community was not well prepared to support military operations in this locale, but given time in the fall and winter of 1990 to put together a capability, the job was done. The Joint Intelligence Center was established during the war with representation from the key intelligence agencies and provided a model of providing crisis support to military operations. Indeed, a permanent National Military Joint Intelligence Center was established shortly after the conflict at the Pentagon and later at all unified commands. Still, the war illuminated problems in disseminating imagery to the field as well as the limitations of U.S. human intelligence capabilities. In addition, a substantial problem arose with competing CIA and military assessments of the damage caused by allied bombing.

The Gates Task Forces

In 1991, after a wrenching confirmation process which provided the first public examination of the analytical process at the CIA, DCI Robert Gates undertook a comprehensive reexamination of the post-Cold War Intelligence Community. The recommendations of 14 separate task forces produced significant change: analysis would be made more responsive to decisionmakers; a formalized requirements process would be established for human source intelligence collection; new offices were created at the CIA to coordinate the use of publicly available ("open source") information and to improve CIA support to the military. The staff of the DCI, which supported him in his Community role, was strengthened. And, after much negotiating about which entities to include, a new Central Imagery Office, under the joint control of the DCI and the Secretary of Defense, was established to coordinate imagery collection and to establish uniform standards for the interpretation and dissemination of imagery to the field.

Boren-McCurdy Legislation

While the Gates task forces were at work, legislation was introduced by the respective Chairmen of the Senate and House intelligence committees to restructure the Intelligence Community. The bills called for the creation of a Director of National Intelligence with authority over the intelligence budget as well as authority to transfer personnel temporarily from one intelligence agency to another. The DNI would continue to establish requirements and priorities for intelligence collection and serve as the President's intelligence adviser. In this regard, the analytical element of the CIA would be transferred under the control of the DNI, leaving the remainder of the CIA to be administered by a separate agency director. The legislation also proposed a National Imagery Agency to coordinate imagery tasking, collection, processing, and dissemination.

Given the actions taken by DCI Gates to implement the results of his task forces, however, the committees did not push for enactment of their alternative proposals. Instead they opted to codify and to clarify the existing statutory framework that had been largely unchanged since 1947. The Intelligence Organization Act of 1992 (enacted as part of the Intelligence Authorization Act for 1993) for the first time defined the Intelligence Community by law, enunciated the three roles of the DCI, set forth the authorities and responsibilities of the DCI in relation to other elements of the Intelligence Community, and articulated the responsibilities of the Secretary of Defense for the execution of national intelligence programs. Among other things, the Secretary was required to consult with the DCI prior to appointing the Directors of the NSA, the NRO,[20] and the DIA.

Congress continued to debate whether the intelligence budget should be declassified. In 1991 and 1992, Congress passed non-binding "Sense of Congress" resolutions urging the President to make public the aggregate funding for intelligence. President Bush declined to do so, as did President Clinton in 1993.

The Vice President's National Performance Review

In 1993, as part of the Clinton Administration's overall effort to "reinvent" government, a team from the Vice President's National Performance Review looked at the Intelligence Community and suggested that several actions be taken to consolidate activities and build a sense of Community in order to be more efficient and to better serve

customers. The review found that the Community was too often drawn apart by the competition for new programs and budget allocations and recommended rotational assignments among agencies as a means of promoting a broader, more collegial perspective. The review's recommendation that the Intelligence Oversight Board be merged into the President's Foreign Intelligence Advisory Board was accomplished by Executive Order in September 1993.

The Ames Spy Case

In February 1994, Aldrich H. Ames, a CIA employee with almost 30 years experience in operations, was charged with spying for the Soviet Union since at least 1985. During this period, he was alleged to have disclosed virtually all of the CIA's active Soviet agents, many of whom were later executed or imprisoned. In May, Ames and his wife pled guilty and were sent to prison.

The ensuing investigations by the CIA Inspector General and by the congressional intelligence committees reported that Ames had exhibited serious personal problems and a penchant for exorbitant spending which should have brought him under security scrutiny. The investigations also highlighted problems in coordinating counterintelligence cases between the FBI and the CIA. Notwithstanding the seriousness of Ames' disclosures and the numerous shortcomings on the part of CIA officers, DCI Woolsey meted out what were perceived as relatively mild disciplinary measures. The confidence of the public and the Congress in the CIA appeared considerably eroded.

In the fall of 1994, new legislation was enacted to improve counterintelligence and security practices across the Intelligence Community, and, in particular, to improve the coordination between the FBI and CIA. In addition, the President created a new bureaucratic framework for handling counterintelligence matters, to include the placement of FBI counterintelligence specialists within the CIA.

The Creation of a New Commission

Even before the Ames case provided the immediate impetus, the congressional intelligence committees anticipated that the Executive branch would conduct a comprehensive review of the Intelligence Community. When this failed to materialize, the Senate committee, and, in particular, its Vice Chairman, Senator John Warner, developed legislation to establish a commission to study the roles and capabilities of intelligence agencies in the post-Cold War era, and to make recommendations for change. The legislation was approved in October 1994, as part of the Intelligence Authorization Act for 1995.

ENDNOTES

1. Former Secretary of State Dean Rusk recalled the 1941 state of the U.S.'s intelligence effort in testimony before a Senate subcommittee: "When I was assigned to G-2 in 1941, well over a year after the war had started in Europe, I was asked to take charge of a new section that had been organized to cover everything from Afghanistan right through southern Asia, southeast Asia, Australia, and the Pacific. Because we had no intelligence organization that had been giving attention to that area up to that time, the

materials available to me when I reported for duty consisted of a tourist handbook on India and Ceylon, a 1924 military attache's report from London on the Indian Army, and a drawer full of clippings from the *New York Times* that had gathered since World War One. That was literally the resources of the G-2 on that vast part of the world a year after the war in Europe started."

2. In 1957, this group was renamed the Bureau of Intelligence and Research.

3. The same Sidney Souers who had been appointed the first DCI by President Truman in January 1946. Souers served as Executive Secretary of the NSC from 1947 to 1950.

4. Although NSC 50 was issued to implement the report's recommendations, DCI Hillenkoetter did not take follow-up action on its numerous recommendations.

5. The same person who proposed the creation of the National Security Council and the CIA in a 1945 report to Navy Secretary Forrestal.

6. The depth and importance of this problem was revealed when President Truman announced that the Soviets had detonated a nuclear device in September 1949. The CIA's only coordinated estimate on the urgent question of when the Soviets would have a nuclear weapon gave three incorrect predictions: 1958, 1955 and 1950–1953, and none of the predictions was accepted by all departments.

7. In its 1955 report, the Second Hoover Commission recognized for the first time the existence of an "intelligence community" within the Government, naming the NSC, CIA, NSA, FBI, Department of State, Army, Navy, Air Force, and the Atomic Energy Commission as its members.

8. Allen Dulles, who had been elevated to DCI in 1953, did not appoint a Chief of Staff, due to his active interest in the operation of the CIA. Instead, he appointed General Lucien Truscott as his deputy to resolve jurisdictional disputes between CIA and the military services, in an attempt to increase his community coordination capabilities.

9. In 1956, the House and Senate Armed Services Committees, and the Senate Appropriations Committee established intelligence subcommittees, and the House Appropriations Committee formed a "special group" under its chairman.

10. The United States Intelligence Board, previously established in the 1950s to serve as the DCI's primary advisory body, was used unevenly by DCIs depending on their interests in Community management.

11. The Intelligence Committee, chaired by the National Security Advisor, consisted of the Attorney General, the Under Secretary of State, the Deputy Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the DCI.

12. CIA officials refused the White House request that the CIA be used to cover-up the Watergate affair.

13. In 1976, Murphy was appointed by President Ford as the first chairman of the newly-formed Intelligence Oversight Board, and as a member of PFIAB.

14. The principal author of these conclusions was reportedly William Casey, later to become DCI.

15. It should also be noted that DCI Colby appointed a study group within CIA, headed by James Taylor, which issued an internal report in October 1975: "American Intelligence: A Framework for the Future." The Taylor study asserted that intelligence needed to become more efficient and effective, and more compatible with our democracy. The study suggested refining the current intelligence system and focused on the role of the DCI, including the relationship with the Secretary of Defense and the Intelligence

Community, arguing that the DCI needed more influence over both substantive judgments and resource management. The report noted that the DCI's responsibilities, but not his authorities, had grown considerably since 1947. The study recommended separating the DCI from CIA (which would be run by its own director), and appropriating funds to the DCI who would allocate them to program managers.

16. This order and succeeding orders issued by President Carter (E.O. 12036, 1978) and President Reagan (E.O. 12333, 1981) listed the following members of the Intelligence Community: CIA, NSA, DIA, DOD reconnaissance offices, INR/State, intelligence elements of Army, Navy, Air Force, Marines, FBI, Treasury, and DOE (then known as the Energy Research & Development Administration). Staff elements of the DCI were added in the Carter and Reagan orders.

17. The other members of the CFI were the Deputy Secretary of Defense for Intelligence and the Deputy Assistant to the President for National Security Affairs. The CFI reported directly to the NSC.

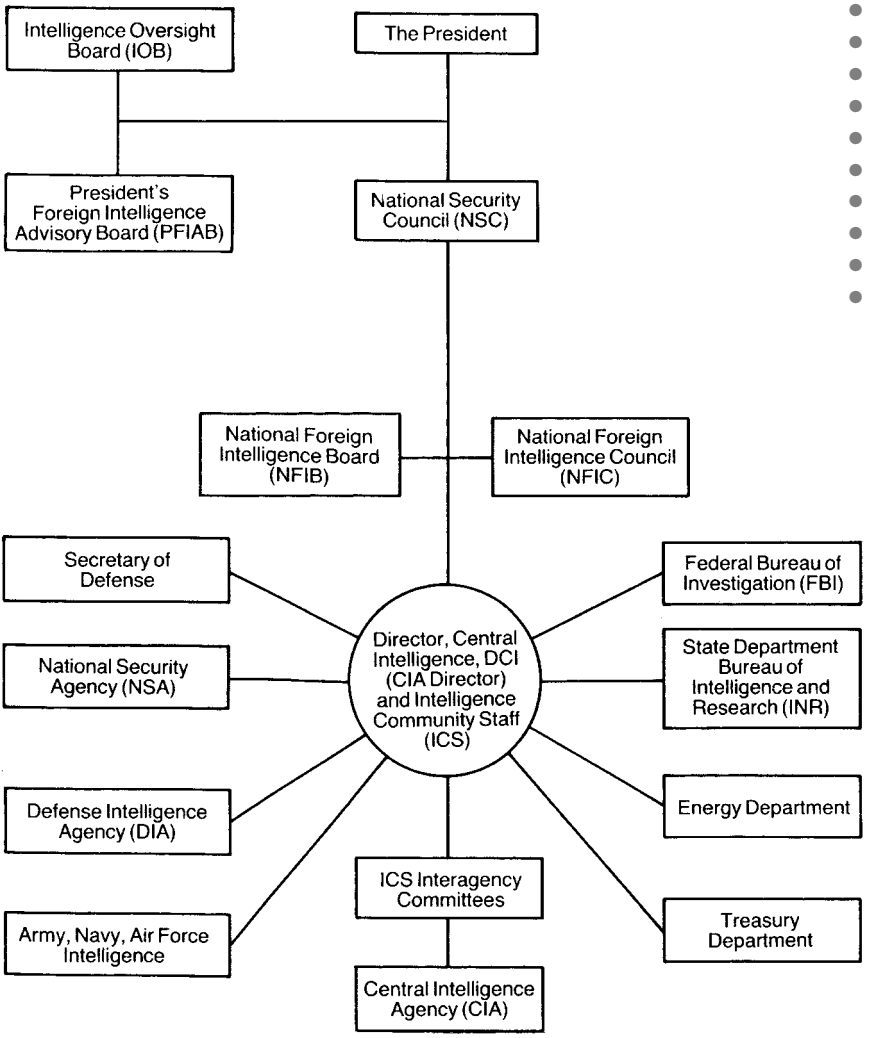
18. Those who thought the DNI must retain a direct management role over the CIA argued that separating the DNI from the CIA would deprive the Director of a strong institutional base and would subject him to more pressure from the policymakers.

19. Neither President Bush nor President Clinton issued executive orders on intelligence that supersede E.O. 12333. It remains in effect.

20. In 1992, as the legislation was under consideration, the President declassified the fact of the NRO's existence.

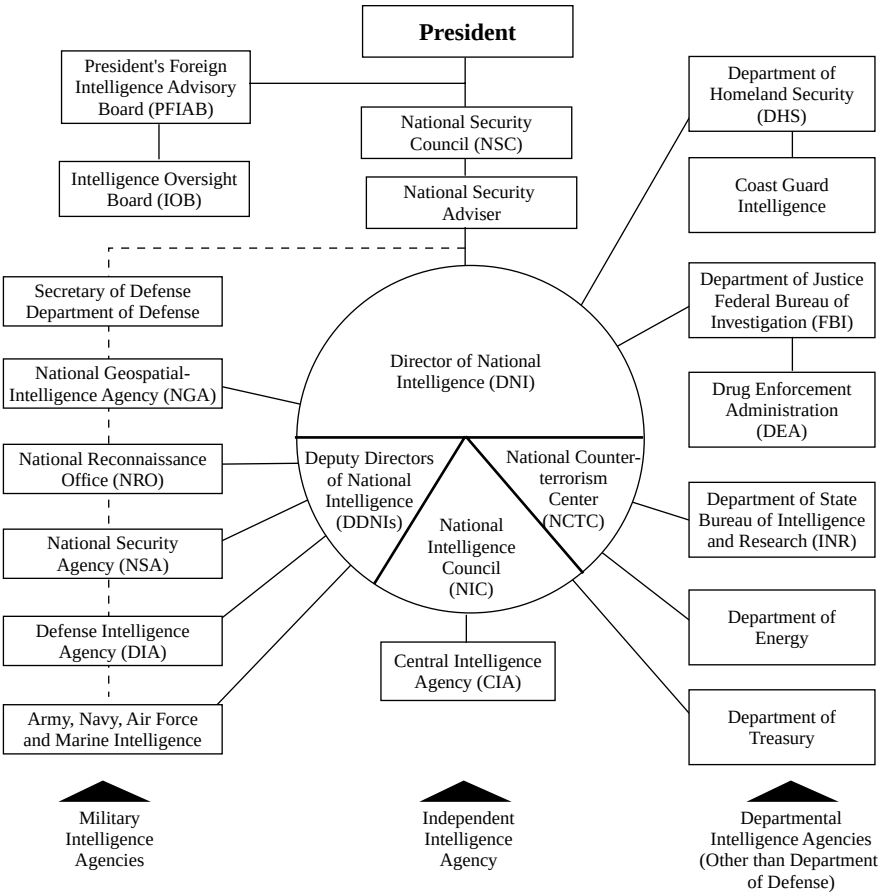
APPENDIX C

THE U.S. INTELLIGENCE COMMUNITY, 1985



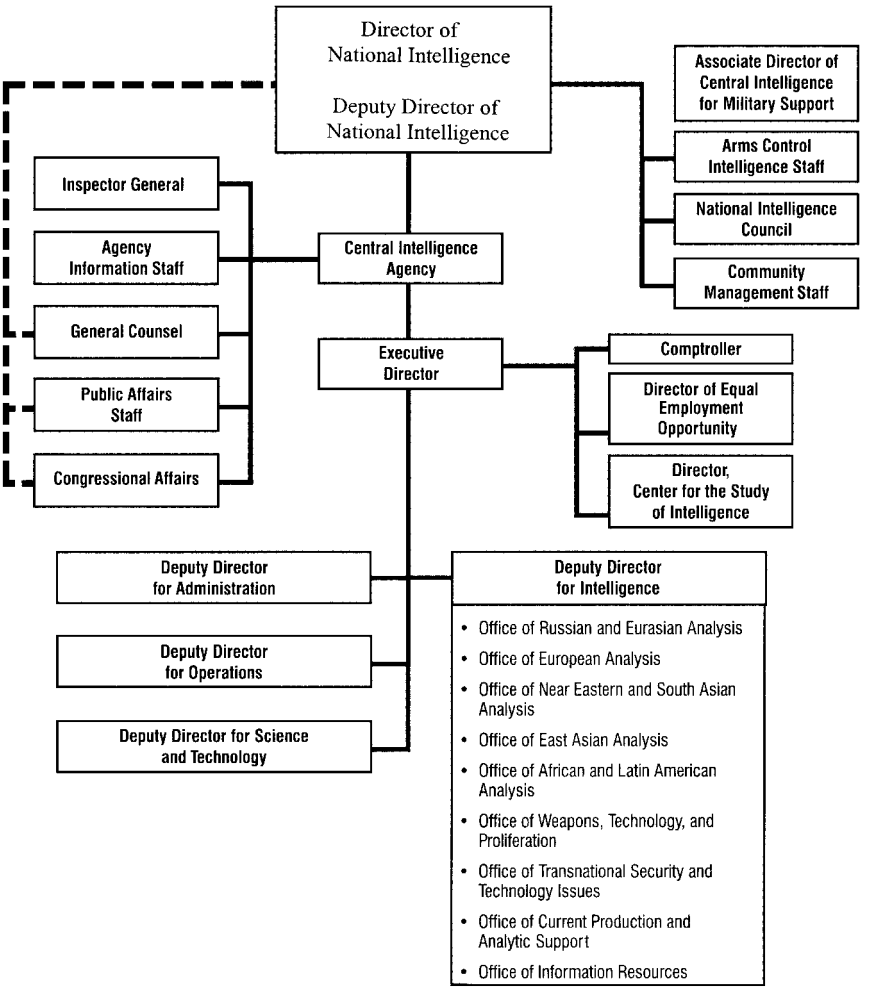
Adapted from Loch K. Johnson, *America's Secret Power* (New York: Yale University Press, 1987), p. 39.

THE U.S. INTELLIGENCE COMMUNITY, 2006



From 1947 to 2005, a Director of Central Intelligence (DCI) led the Intelligence Community, rather than a Director of National Intelligence (see the previous figure). The Department of Homeland Security and the Coast Guard did not become part of the IC until 2003; and the Drug Enforcement Administration, in 2006. For a more detailed organizational diagram for the Office of the Director of National Intelligence, see: http://www.dni.gov/aboutODNI/organization.htm

THE ORGANIZATION OF THE CENTRAL INTELLIGENCE AGENCY, WITH DETAILS ON THE DIRECTORATE FOR INTELLIGENCE—HOME OF THE CIA'S ANALYSTS



Adapted from "Analysis: Directorate of Intelligence in the 21st Century," *Strategic Plan*, Directorate of Intelligence, Central Intelligence Agency (Washington, D.C.: August 1996), p. i.

APPENDIX D

AN AERIAL PHOTOGRAPH OF THE CENTRAL INTELLIGENCE AGENCY, 1996

Photo courtesy of the CIA Office of Public Affairs, 2006.

APPENDIX E

LEADERSHIP OF THE U.S. INTELLIGENCE COMMUNITY, 1947–2006

DIRECTORS OF CENTRAL INTELLIGENCE

Rear Adm. Sidney W. Souers, USNR	23 January 1946–10 June 1946
Lt. Gen. Hoyt S. Vandenberg, USA	10 June 1946–1 May 1947
Rear Adm. Roscoe H. Hillenkoetter, USN	1 May 1947–7 October 1950
Gen. Walter Bedell Smith, USA	7 October 1950–9 February 1953
The Honorable Allen W. Dulles	26 February 1953–29 November 1961
The Honorable John A. McCone	29 November 1961–28 April 1965
Vice Adm. William F. Raborn, Jr., USN (Ret.)	28 April1965–30 June 1966
The Honorable Richard Helms	30 June 1966–2 February 1973
The Honorable James R. Schlesinger	2 February 1973–2 July 1973
The Honorable William E. Colby	4 September 1973–30 January 1976
The Honorable George Bush	30 January 1976–20 January 1977
Adm. Stansfield Turner, USN (Ret.)	9 March 1977–20 January 1981
The Honorable William J. Casey	28 January 1981–29 January 1987
The Honorable William H. Webster	26 May 1987–31 August 1991
The Honorable Robert M. Gates	6 November 1991–20 January 1993
The Honorable R. James Woolsey	5 February 1993–10 January 1995
The Honorable John M. Deutch	10 May 1995–15 December 1996
The Honorable George J. Tenet	11 July 1997–11 July 2004
The Honorable Porter J. Goss	24 September 2004–20 April 2005

DIRECTOR OF NATIONAL INTELLIGENCE

The Honorable John D. Negroponte	20 April 2005–

CHAIRS, U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE

1976–77	Daniel K. Inouye, Democrat, Hawaii
1977–81	Birch Bayh, Democrat, Indiana
1981–85	Barry Goldwater, Republican, Arizona
1985–87	David Durenberger, Republican, Minnesota
1987–93	David L. Boren, Democrat, Arizona
1993–95	Dennis DeConcini, Democrat, Arizona
1995–97	Arlan Specter, Republican, Pennsylvania
1997–01	Richard C. Shelby, Republican, Alabama
2001–02	Bob Graham, Democrat, Florida
2002–	Pat Roberts, Republican, Kansas

CHAIRS, HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

1977–85	Edward P. Boland, Democrat, Massachusetts
1985–87	Lee H. Hamilton, Democrat, Indiana
1987–89	Louis Stokes, Democrat, Ohio
1989–91	Anthony C. Beilenson, Democrat, California
1991–93	Dave McCurdy, Democrat, Oklahoma
1993–95	Dan Glickman, Democrat, Kansas
1995–97	Larry Combest, Republican, Texas
1997–2004	Porter J. Goss, Republican, Florida
2004–	Peter Hoekstra, Republican, Michigan

MEMBERSHIP, SENATE SELECT COMMITTEE ON INTELLIGENCE, 2006

Republicans	*Democrats*
Pat Roberts, Kansas, Chair	John D. Rockefeller, IV, West Virginia, Vice Chair
Orrin G. Hatch, Utah	Carl Levin, Michigan
Mike Dewine, Ohio	Dianne Feinstein, California
Christopher S. Bond, Missouri	Ron Wyden, Oregon
Trent Lott, Mississippi	Evan Bayh, Indiana
Olympia J. Snowe, Maine	Barbara A. Mikulski, Maryland
Chuck Hagel, Nebraska	Russell D. Feingold, Wisconsin
Saxby Chambliss, Georgia	

MEMBERSHIP, HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE, 2006

Republicans

Peter Hoekstra, Michigan, Chair
Ray LaHood, Illinois
Terry Everett, Alabama
Elton Gallegly, California
Heather Wilson, New Mexico
Jo Ann Davis, Virginia
Mac Thornberry, Texas
John McHugh, New York
Todd Tiahrt, Kansas
Mike Rogers, Michigan
Rick Renzi, Arizona
Darrell Issa, California

Democrats

Jane Harman, California, Vice Chair
Alcee L. Hastings, Florida
Silvestre Reyes, Texas
Leonard L. Boswell, Iowa
Robert E. (Bud) Cramer, Jr., Alabama
Anna G. Eshoo, California
Rush D. Holt, New Jersey
C.A. Dutch Ruppersberger, Maryland
John Tierney, Massachusetts

APPENDIX F

SHERMAN KENT ON "THE NEED FOR AN INTELLIGENCE LITERATURE"

Published in the first issue of Studies in Intelligence *in September 1955, this essay reveals why Sherman Kent believed that intelligence had become a profession and explained the kind of literature that this learned profession needed and deserved.*

In most respects the intelligence calling has come of age. What has happened to it in the last fourteen years is extraordinary. Maybe our present high is not so extraordinary as our low of 1941. In that day the totality of government's intelligence resources was trifling. We knew almost nothing about the tens of thousands of things we were going to have to learn about in a hurry. As emergencies developed we found ourselves all too reliant upon British intelligence. Many of us recall important studies issued by US intelligence organizations which were little more than verbatim transcripts of the British ISIS reports.

In 1941, the number of people who had had prior intelligence experience and who at the same time were available for new government assignments in intelligence was very small. There were few in Washington who could give any guidance as to how to go about the business at hand. What intelligence techniques there were, ready and available, were in their infancy. Intelligence was to us at that period really nothing in itself; it was, at best, the sum of what we, from our outside experience, could contribute to a job to be done. It did not have the attributes of a profession or a discipline or a calling. Today things are quite different.

Let me briefly note the principal assets of today' intelligence community. To begin with, we are at strength. Perhaps we are not as strong as the present volume of work requires, but by and large we have the staff to do the man-sized job before us.

Source: Donald P. Steury, ed., *Sherman Kent and the Board of National Estimates: Collected Essays*, History Staff, Center for the Study of Intelligence, Central Intelligence Agency, Washington, D.C. (1994), pp. 13–19.

Again, we are not novices at our businesses; we have a lot of experience behind us. We are officered and manned by a large number of people with more than a decade of continuous experience in intelligence, and who regard it as a career to be followed to retirement. By now we have orderly file rooms of our findings going back to the war, and we have methods of improving the usefulness of such files. We have orderly and standardized ways of doing things. We do most things the right way almost automatically. We have developed a host of new and powerful overt and covert techniques which have increased the number of things we can and do find out about. Most important of all, we have within us a feeling of common enterprise and a good sense of mission.

With these assets, material and experiential, intelligence is more than an occupation, more than a livelihood, more than just another phase of government work. Intelligence has become, in our own recent memory, an exacting, highly skilled profession, and an honorable one. Before you can enter this profession you must prove yourself possessed of native talent and you must bring to it some fairly rigorous pretraining. Our profession like older ones has its own rigid entrance requirements and, like others, offers areas of general competence and areas of very intense specialization. People work at it until they are numb, because they love it, because it is their life, and because the rewards of professional accomplishment.

Intelligence today is not merely a profession, but like most professions it has taken on the aspects of a discipline: it has developed a recognized methodology; it has developed a vocabulary; it has developed a body of theory and doctrine; it has elaborate and refined techniques. It now has a large professional following. What it lacks is a literature. From my point of view this is a matter of greatest importance.

As long as this discipline lacks a literature, its method, its vocabulary, its body of doctrine, and even its fundamental theory run the risk of never reaching full maturity. I will not say that you cannot have a discipline without a literature, but I will assert that you are unlikely to have a robust and growing discipline without one.

Let me be clear about this literature that we lack. First, let me say what I do *not* mean that we are lacking. I do not mean the substantive findings of intelligence. Manifestly, I do not mean those thousands of words we disseminate each day about past, present, and probable future goings on all over the world. I do not refer to the end product of all of our labors. We produce a great deal of this sort of literature and possibly we produce too much of it. It is not that literature that I am talking about. What I am talking about is a literature dedicated to the analysis of our many-sided calling and produced by its most knowledgeable devotees. The sort of literature I am talking about is of the nature of house organ literature, but much more. You might call it the institutional mind and memory of our discipline. When such a literature is produced, it does many things to advance the task.

The most important service that such a literature performs is the permanent recording of our new ideas and experiences. When we record we not only make possible easier and wider communication of thought, but we also take a rudimentary step towards making our findings cumulative. We create a stock of relatively imperishable thinking that one man can absorb without coming into personal contact with its originator and against which he can weigh and measure his own original ideas. His large or small addition to the stock enriches it. The point is reached where an individual mind, capable of using the stock, can in a day encompass the accumulated wisdom of man-decades of reflection and action.

Consider such disciplines as chemistry or medicine or economics and ask yourself where they would be today if their master practitioners had committed no more to paper

than ours. Where would we be if each new conscript to medicine had to start from scratch with no more to guide him than the advice of fellow doctors and his own experience? Where would we be in medicine if there was nothing to read and nothing to study, no textbooks, no monographs, no specialized journals, no photographs, no charts, no illustrations, no association meetings with papers read and discussed and circulated in written form? Where would we be if no one aspired to the honor of publishing an original thought or concept or discovery in the trade journals of his profession? It is not impossible that bloodletting would still be considered a valuable panacea and exposure to night swamp air the specific for syphilis.

The point is that in the last few centuries we have accumulated an enormous amount of knowledge. And the fact that this accumulation has taken place since the discovery of printing from movable type is by no means merely coincidental. The translation of new thought into words, and the commission of words to the permanence of print, more than anything else has made possible a progressive and orderly advance in all disciplines and all areas of learning.

In our calling, I am saying, we do not do enough of it. To be sure we do do some writing. We have produced a good many training manuals of one sort or another. We have done a good bit of chronicling of interesting case studies with an educational end in view. We have made transcripts of oral presentations at training centers. If you ransacked the "libraries" of intelligence schools you would find quite an amount of written material. Even so there is a very considerable difference between this volume of written material and the systematic professional literature I am talking about.

It is hard to define such a literature, and I will not try to do it in a sentence or two. As a starter I will note what I think to be three important aspects of it. To begin with, *the literature I have in mind will deal with first principles.* A portion of it will certainly have to deal with the fundamental problem of what we are trying to do. What is our mission? And as soon as that question is submitted to careful analysis, there is no telling what will emerge. One thing I think is certain: that is, that we have many more than a single mission and that many of us have been confused not only about the number and character of the many missions, but also how each relates to the others.

Another first principle that will have to be elaborated on is how we are going about our mission—what is our method? Here again we will find out, when the question is systematically answered, that there is not a single method, but that there are dozens of methods; and from further examination or discussion we will confront a good many new concepts which will speed our task and enrich our product.

Let no one feel either that we are necessarily sure of the nature of our first principles or that dispassionate examination of them would be a waste of time. In recent months the intelligence community has had to wrestle with such fundamental concepts as "national intelligence objectives" and the criteria for the selection of such objectives, the nature of "warning," the role of "indications," and so on. The results of these discussions have been generally praiseworthy, but the amount of time consumed and the consequent delay of important decisions quite otherwise. An analogous situation might be a consultation of surgeons deadlocked on a discussion of the nature of blood, preliminary to handling the emergency case presently on the operating table.

This takes me to a second thing which I would expect from a systematic literature of intelligence: *a definition of terms.* Hastily let me add that I am not proposing that we write a dictionary. Words like "liberalism" and "democracy" require the equivalent of scores of

dictionaries, or scores of shelves of dictionaries. You cannot define those as you define "paper" and "ink." So it is with our own words that stand for complicated concepts—such as "evaluation," "indicator," "capability," "estimates," and so on. As of today we use these words easily and often—yet one wonders if they are always understood in exactly the way intended. For example, we would be almost tongue-tied without the word "capability"; we use it perhaps more often than any other of our semi-technical words. Yet a little reflection on the matter shows that we use it indiscriminately to mean one of three quite different things: a feasible course of action, a raw strength, and a talent or ability. Can we be sure that we are always conveying an intended sense?[1]

If we do not rigorously define our terms we are likely to find ourselves talking at cross purposes; and such discussion, we all realize, risks being more of a fruitless dispute than an elevated debate. This takes me to a third point.

The literature I have in mind will, among other things, be an *elevated* debate. For example, I see a Major X write an essay on the theory of indicators and print it and have it circulated. I see a Mr. B brood over this essay and write a review of it. I see a Commander C reading both the preceding documents and reviewing them both. I then see a revitalized discussion among the people of the indicator business. I hope that they now, more than ever before, discuss indicators within the terms of a common conceptual frame and in a common vocabulary. From the debate in the literature and from the oral discussion, I see another man coming forward to produce an original synthesis of all that has gone before. His summary findings will be a kind of intellectual platform upon which the new debate can start. His platform will be a thing of orderly and functional construction and it will stand above the bushes and trees that once obscured the view. It will be solid enough to have much more built upon it and durable enough so that no one need get back in the bushes and earth to examine its foundations.

Now if all this sounds ponderous and a drain on time, I can only suggest that, so far, we of the Western tradition have found no faster or more economical way of advancing our understanding. This is the way by which the Western world has achieved the knowledge of nature and humanity that we now possess.

These are only three things that I would expect from this literature. There are many others. It could and should record such things as new techniques and methods, the history of significant intelligence problems and accomplishments, the nature of intelligence services of other countries, and so on. But the three items that I have singled out remain the most important.

There are perils of going forward in our profession without laying down such a literature. First, there are the obvious perils of denying our calling the advantages I have discussed above. There is, however, another peril and one we should heed for strictly utilitarian reasons. As things now stand, we of the intelligence profession possess practically no permanent institutional memory. Our principal fund of knowledge rests pretty largely in our heads; other funds of knowledge are scattered in bits through cubic miles of files. What happens to our profession if we are demobilized as we were after the two world wars? What happens to it if our heads and files find themselves in the middle of a nuclear explosion? The answer, I fear, is that a new beginning will have to be

[1] [*Studies*] Editor's Note: In our next monograph, one of Mr. Kent's colleagues, Abbot Smith, takes up precisely this problem in his article "Capabilities in National Estimates" [*Studies in Intelligence* (January 1956)].

made virtually from scratch. Most of what we know will go when we go; only a very small part will be left behind. A literature of intelligence is a reasonable insurance policy against repetition of two demobilizations of intelligence that have occurred within our memory.

In highlighting the desirability of producing a literature of intelligence and stressing the perils of not producing one, I do not wish to seem to close my eyes to problems and difficulties.

The first of these is probably the matter of security. One can expect the question: "Do you want to put all the secrets of the profession in writing and bind them up in one great book so that your enemy's success with a single target will at once put him abreast of you?" The answer comes in two parts. In the first place, many of the most important contributions to this literature need not be classified at all. They could be run in the daily press and our enemies would get no more good from them than from the usual run of articles published in our professional journals. Surely the enemy would benefit in some degree; he would benefit as he presently does from his reading of *The Infantry Journal* or *Foreign Affairs.* On the other hand, another type of contribution would deal with delicate trade secrets and would have to be classified. But is this reason not to write or circulate it? Every day we have to decide on the correct security procedure with respect to sensitive materials. Why should the literature at instance be necessarily more delicate or sensitive than the last cable from Paris, and why should its proper handling be more difficult or dangerous? In this case, as in the more familiar one of the sensitive report, we must again equate the value of exposing many minds to a problem with the increasing danger of disclosure. The plain fact is that "security" and the advance of knowledge are in fundamental conflict. The only reason we get anywhere is because we do not demand either perfect security or unlimited debate about secrets of state. We do get somewhere because the necessity for compromise at both ends is well and fully understood.

There is another difficulty and a very practical one. How is such a literature to be written if most or all of the potential authors are practicing members of the profession, already burdened with seemingly higher priority tasks? I know of no magic formula by which a man can do two things at once. The question that we face is the familiar one of priorities. Surely one of the guiding principles to a solution is the desirability of investing for the future. Taking Mr. X off the current task and giving him the time to sort out his thoughts and commit them to paper will more than repay the sacrifice if what Mr. X puts down turns out to be an original and permanent contribution. If it buttons up a controversial matter and precludes thousands of hours of subsequent discussion, the cause has been well served. It has been well served even though one of Mr. X's would-be-consumers had to get along without his advice on another matter. What we are faced with in this case is nothing more complicated than the value and pain of capital formation.

A third problem. How may the Mr. X's be paid for work time spent in the creation of this literature? If what has gone before is the fact and the Mr. X's of the calling are really creating intelligence capital, then it seems to me that they are entitled to their wage exactly as if engaged upon their regular assignments. Indeed, in logic, if what Mr. X produces contributes to the solution of the next hundred problems, he should be paid more than if he spent his time merely solving the single assigned problem before him.

Beyond these rather fundamental matters, there are hundreds of other problems. If a large proportion of the Mr. X's are sure to come from intelligence staffs, where do they

work? Are they to have secretarial help? Will they keep regular hours? Must they be in residence? How will their findings be reproduced? How will they be circulated? What editorial controls will be exercised over their output? These are really easy questions. The hard ones are to find the Mr. X's in the first place, and to induce them to undertake the most difficult job of all: original creative writing.

APPENDIX G

THE ASPIN-BROWN COMMISSION ON THE PURPOSE AND CHALLENGES OF INTELLIGENCE

INTRODUCTION

BACKGROUND LEADING TO THE CREATION OF THE COMMISSION

In the euphoria the followed the collapse of communist regimes in Eastern Europe in 1989 and the dissolution of the Soviet Union in 1991, some wondered whether intelligence agencies would still be necessary. Gone was the Cold War's military threat to U.S. survival, and no comparable threat appeared on the horizon.

It was soon apparent, however, that significant, if lesser, threats remained. The 1991 Persian Gulf War quelled, for the time being, one such threat, and also signaled an expanded role for intelligence in modern warfare. Never before had intelligence been so closely integrated into combat operations with such devastating impact. The deployment of U.S. military forces into unanticipated situations in Somalia, Rwanda, and Haiti also imposed new demands on intelligence agencies. The discovery by U.S. intelligence in 1992 of the beginnings of a nuclear weapons program in North Korea reminded Americans of the need for continued vigilance.

But if intelligence was still needed, its focus remained unclear. Some of the rationales offered to the public, such as environmental intelligence, suggested that intelligence agencies might be looking for new missions to justify their existence. The uncertainty felt by the public was reflected to some degree in the reduced resource commitment that Congress was willing to make to the intelligence function. The dramatic rise in funding

---

Source: "Preparing for the 21st Century: An Appraisal of U.S. Intelligence," *Report of the Commission on the Roles and Capabilities of the United States Intelligence Community* (the Aspin-Brown Commission), Washington, D.C. (March 1, 1996), pp. 1–35.

that had taken place in the 1980s came to an abrupt end in 1989, and it steadily decreased thereafter. Across-the-board personnel reductions were imposed as well.

At the same time, intelligence operations were being increasingly revealed to the public, and not always in flattering terms. The 1991 confirmation hearings of Robert Gates involved a wrenching examination of whether CIA analysis had been distorted for political purposes during the Reagan Administration. In the meantime, the public learned that most of the CIA's agents in Cuba and East Germany during the latter stages of the Cold War had, in fact, been controlled by the other side.

Within Congress, there was an early, but unsuccessful, attempt to direct organizational reform. In 1992, the chairmen of both congressional intelligence committees introduced similar legislation calling for major restructuring of intelligence agencies under a "Director of National Intelligence." At the same time, then DCI Gates instituted a series of internal task forces that produced recommendations for reform in a number of areas. While the work of these task forces did not result in major structural change, they did represent a substantial effort to adjust the operations of the Intelligence Community in the wake of the Cold War. In the face of the new DCI's actions, Congress backed away from more radical structural change and enacted legislation in 1992 that largely codified the authorities and responsibilities of the DCI under Executive branch policy.

After the 1992 presidential elections, a new DCI, R. James Woolsey, was appointed and continued many of the Gates reforms. The ensuing period did not, however, produce major structural change.

In the meantime, the series of revelations damaging to the CIA continued. Two lawsuits—one a class action suit by several hundred present and former female CIA employees—were filed alleging past sexual discrimination by the Agency. Both received extensive coverage in the media.

Then, in February 1994, a 30-year employee of the CIA, Aldrich H. Ames, and his wife, were arrested for spying for the Soviet Union and later for Russia. As information about the case began to surface, it became clear that Ames' disclosures, beginning in 1985, had resulted in monumental damage to the core of the Agency's operations—collection against the former Soviet Union. Ten of its most important Soviet sources had been executed; others were imprisoned. It also came to light that CIA had had considerable information indicating a potential security problem with Ames but had failed to pursue it adequately and had failed to bring the FBI into the case until late in the process.

When it came time to discipline those responsible for these failures, DCI Woolsey issued what were widely perceived as relatively mild punishments. The public began to question both the competence of the CIA to carry out its mission and the degree to which the management and employees of the Agency were held accountable.

As the implications of the Ames case were beginning to dawn on the public, it came to light that another intelligence agency, the National Reconnaissance Office, had built a new headquarters building in suburban Virginia under the cover of one of its contractors at a cost of over $300 million. While the oversight committee in the House of Representatives said it had been advised of the project, members of the Senate oversight committee contended they had not been adequately informed. In any event, the public perception was that of an intelligence agency, acting in secret and without adequately informing the Congress, building a costly headquarters for itself at a time when the rest of government

was drawing down. Reacting to the episode, Congress enacted legislation requiring specific notification of any new construction costing $500,000 or more.[1]

It was this background—

- the uncertainty with respect to what intelligence agencies should do in the wake of the Cold War;
- the perceived lack of a serious and comprehensive effort to bring about reform;
- the discomfort with the level of resources still committed to intelligence; and
- instances of apparent incompetence, mismanagement, and unaccountability among intelligence agencies,

that prompted the Congress to consider creating a commission on intelligence.

When the intelligence authorization bill came to the floor of the Senate in August 1994, an amendment proposing a bipartisan "Commission on the Roles and Capabilities of the U.S. Intelligence Community" was offered by the leaders of the Senate oversight committee. In the ensuing debate, Senators repeatedly cited the need for a new consensus where intelligence was concerned and the need to revalidate the intelligence function.[2]

The House of Representatives agreed to the Senate proposal with minor modifications. Conferees on the measure stated it was their intent "to produce credible, independent, and objective review of the intelligence community."[3] The President signed the bill into law on October 14, 1994.[4]

THE COMMISSION AND ITS WORK

The Commission on the Roles and Capabilities of the United States Intelligence Community was charged with reviewing "the efficacy and appropriateness" of U.S. intelligence activities in the "post-cold war global environment" and with preparing a report of its findings and recommendations to the President and the Congress. The law creating the Commission set forth 19 separate issues to be considered as part of its overall review.

A Commission of 17 members was established, consisting of nine members appointed by the President and eight appointed by the congressional leadership. Of the congressional appointments, four were to be appointed by the House (two by the Speaker and two by the Minority Leader) and four by the Senate (two by the Majority Leader and two by the Minority Leader). One of the two appointments made by each congressional leader had to be a sitting Member of their respective body. Of the nine presidential appointments, no more than five could be from the same political party, and no more than four could have previous intelligence experience. Thus, the Commission was designated to be a bipartisan body which brought to bear the perspectives of the Executive and Legislative branches as well as that of the private sector.

On November 29, 1994, then Speaker of the House Thomas Foley appointed Representative Norman D. Dicks of Washington and Tony Coelho of Virginia to the Commission.

---

[1] Intelligence Authorization Act For Fiscal Year 1995, § 602, 50 U.S.C. § 403–2b (Supp. 1995).

[2] 140 Cong. Rec. S11379–11389 (daily ed. Aug. 12, 1994). The amendment passed by a vote of 99–0.

[3] H.R. Rep. No. 103–753, 103d Cong., 2d Sess. 65, reprinted in 1994 U.S.C.C.A.N. 2751, 2773.

[4] Intelligence Authorization Act For Fiscal Year 1995, tit. IX, 50 U.S.C. § 401 note (Supp. 1995).

The following day, Senate Majority Leader George Mitchell appointed Senator J. James Exon of Nebraska and Wyche Fowler, Jr., of Georgia. On December 20, 1994, House Minority Leader Robert Michel appointed Representative Porter J. Goss of Florida and Robert E. Pursley of Connecticut to the Commission, and, on January 4, 1995, Senate Minority Leader Robert Dole appointed Senator John Warner of Virginia and David H. Dewhurst of Texas.

On February 3, 1995, President Clinton announced his appointments: Les Aspin of Wisconsin; Warren B. Rudman of New Hampshire; Zoë Baird of Connecticut; Ann Z. Caracristi of Washington, D.C.; Anthony S. Harrington of Washington, D.C.; Lew Allen, Jr. of California; Stephen Friedman of New York; Robert J. Hermann of Connecticut; and Paul D. Wolfowitz of Maryland. Commissioners Aspin and Rudman were designated Chairman and Vice Chairman, respectively.[5] (A brief biographical statement of each member of the Commission can be found at Appendix G.)

The first meeting of the Commission took place on February 3, 1995. The Commission selected a staff director and established a meeting schedule for the forthcoming year. It officially began operations on March 1, 1995.

The Commission held regular monthly meetings, ordinarily two days in length, from March through December, 1995. Early meetings consisted of briefings by the Intelligence Community to educate the Commission on current organization and operations. These were followed by sessions with current and former users of intelligence, and by additional meetings with other knowledgeable persons, to discuss the strengths and weaknesses of the existing system and ideas about how various aspects of the intelligence business might be changed. In all, 84 witnesses provided formal testimony. (A list of the persons who appeared before the Commission can be found at Appendix C.)

Commission members supplemented these formal meetings with visits to intelligence facilities and military commands in the United States and overseas, as well as visits to a number of countries with which the United States has cooperative relationships in the intelligence area, to compare U.S. arrangements for intelligence with those of other governments and to explore further burdensharing, as provided by the Commission's charter.

To elicit additional opinion, the Commission staff conducted over 200 interviews of present and former government officials and knowledgeable persons from the media, academia, and industry. (A list of those interviewed by the staff can be found at Appendix D.) Individual Commissioners and the staff also received numerous factual briefings by representatives of the Intelligence Community.

The Commission also reviewed earlier studies of the Intelligence Community and received a wide range of opinion from private citizens, government contractors, professional associations, and other groups in the form of written statements, letters, articles, books, conference proceedings, and other materials. The Executive branch supplied voluminous documentary material.

In early May, separate task forces were formed to examine particular topics and make recommendations to the Commission as a whole. Commissioner Friedman led a task force on organization; Commissioner Baird, on law enforcement and intelligence; Commissioner Caracristi, on analysis; Commissioner Allen, on budget; and Commissioner Hermann, on space.

[5] At the invitation of Chairman Aspin, one member of the President's Foreign Intelligence Advisory Board (PFIAB), Maurice Sonnenberg, also a member of the Commission on Protecting and Reducing Government Secrecy, served as a senior adviser to the Commission and took an active role in its work. Two other members of the PFIAB, Lois Rice and Sidney Drell, participated in some meetings.

On May 21, 1995, almost four months into its work, the distinguished Chairman of the Commission, Les Aspin, died unexpectedly of a stroke. Commissioners Rudman and Harrington served as interim Chairman and Vice Chairman, respectively, until the President appointed Dr. Harold Brown of California to succeed Mr. Aspin as Chairman on July 13, 1995. Upon Dr. Brown's appointment, Mr. Rudman resumed his position as Vice Chairman.

On June 6, 1995, the Commission provided a detailed work plan, outlining the scope of its inquiry, to the congressional intelligence committees.

Beginning in September 1995, the Commission began to narrow its focus to particular issues and discuss possible options for dealing with them. Reports from the task forces were considered. By December, consensus had formed on most issues, and drafting of the Commission's report began. The Commission met several times in January and February, 1996, to consider drafts of the report, and on February 2, 1996, by unanimous vote, approved its submission to the President and the Congress.

WHAT IS "INTELLIGENCE?"

Before one can assess the "efficacy and appropriateness" of U.S. intelligence activities in the post-Cold War era, it is essential to appreciate what distinguishes "intelligence" from other areas of government activity and how intelligence fits into the business of government.

Although "intelligence" is defined in law and Executive order,[6] neither conveys a very clear understanding of the term. The Commission believes it preferable to define "intelligence" simply and broadly as information about "things foreign"—people, places, things, and events—needed by the Government for the conduct of its functions. Generally speaking, "intelligence" refers to information about "things foreign" that is not available to the Government through conventional means—in other words, to information collected by "secret" or clandestine means. But the work of "intelligence" also involves collecting and analyzing information available through conventional means to the extent needed to understand what is otherwise gathered by "secret" means.

Thus, "intelligence" may be contained in or derived from:

- publicly available sources, including foreign and domestic broadcast and print media, government or private publications, and information available over computer networks;
- personal observation or photographs taken by a person who is physically located at a particular point of interest;
- privileged communications that U.S. Government officials have with their counterparts in other governments or international organizations (which may contain information that is not publicly available);

[6] "Intelligence" is defined in 50 U.S.C. 401a to include foreign intelligence and counterintelligence. "Foreign intelligence" is defined as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons." The term "counterintelligence" is defined as "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."

- photographs taken from air or space of areas that are otherwise inaccessible to persons on the ground;
- the interception of electronic signals or emanations, or the measurement of the physical attributes of things on the ground or in the air; or
- persons who have access to places, persons, or things that are not otherwise available.

Every agency of the U.S. Government whose functions require involvement with foreign governments, entities, or persons—from the Department of State to the Department of Agriculture—collects and analyzes information needed to perform those functions. Typically, such information is gleaned from public sources available to these agencies and from their contacts with foreign counterparts and other substantive experts.

To acquire information about "things foreign" that is not obtainable through these conventional channels, federal agencies generally rely upon "intelligence agencies" that have capabilities and authorities not available to other federal agencies. Some cabinet departments have "intelligence agencies" as subsidiary elements, e.g. the Defense Intelligence Agency within the Department of Defense. Other federal agencies rely upon intelligence agencies that are either independent, like the Central Intelligence Agency (CIA), or belong to other departments.

Intelligence agencies have been created for a variety of reasons. One is cost. Sophisticated technical capabilities, such as satellite reconnaissance, are simply too expensive for every federal agency to have its own. Some intelligence agencies were created to centralize control over activities that were especially sensitive (e.g. running human agents in foreign countries) to facilitate protection of these activities, and to prevent political embarrassment to the United States. Other elements were created to provide analytical objectivity or responsiveness. Some, including the CIA, were created for a combination of these reasons.

Whatever skills or capabilities they might contribute, intelligence agencies, as a whole, have historically shared a common purpose: to collect information that is not otherwise available to the Government, combine it with information that is available, and produce analysis based upon both kinds of sources for the benefit of the Government. Put another way, intelligence agencies have attempted to provide the Government with information and insight it would not otherwise receive, to reduce the uncertainty of decisionmaking.

The President and his chief defense and foreign policy advisers are usually seen as the principal users of intelligence information. In fact, literally tens of thousands of users belonging to an array of federal agencies (and their contractor support base) have daily access to intelligence information. From the diplomat or trade specialist conducting negotiations, to the Pentagon analyst designing military force structures, to commanders in the field who must deploy and target highly sophisticated weapons, to the scientist developing the latest military hardware, intelligence is routinely factored into their decisionmaking. The value of this information to particular users will necessarily depend on its accuracy, its relevance, and its timeliness.

Ultimately, the user is left to make a decision based on the information available. Not infrequently, his or her chosen course of action is dictate by considerations other than the judgments reached by intelligence agencies. This does not mean that intelligence has "failed." While the value of intelligence is obviously greatest when it provides the basis for action by a particular user, it also has value as part of a decisionmaking process

repeated hundreds, if not thousands, of times daily by employees and contractors of the Government.

Intelligence has been a function of the Government literally since the beginning of the Republic. George Washington put intelligence to decisive military use during the American Revolution, and when he became President, persuaded Congress to create a special fund from which intelligence operations could be financed. Intelligence has been an integral part of U.S. military operations ever since. Both the Union and the Confederacy used intelligence extensively during the Civil War. During the 1880s, intelligence was formally institutionalized as part of U.S. peacetime military planning. The first advanced signals intelligence capability was established just prior to World War I. World War II spurred far more substantial growth as the need to support U.S. combat forces in Europe and the Pacific necessitated the creation of new capabilities as well as partnerships with allied countries. A detailed summary of the historical evolution of U.S. intelligence from Washington's presidency the present day is included at Appendix A. It demonstrates that while intelligence came of age during the Cold War era, it has to some degree been a function of the U.S. Government since its very inception.

THE COMMISSION'S REPORT

The mandate of the Commission was to produce a report that dealt with the roles and capabilities of intelligence agencies. It was not chartered to perform an oversight inquiry into alleged improprieties of wrongdoing. In assessing those roles and capabilities, the Commission attempted to limit itself to overarching issues. Given the limited amount of time and resources as its disposal, there was no practical alternative.

Many perceived problems were brought to our attention by the hundreds of people who communicated with us. On examination, some did not appear problems at all, or, if they were problems, intelligence agencies appeared to be taking appropriate steps to deal with them. Similarly, the Commission was presented with a wide range of suggested solutions. The Commission considered them all, from the most extreme (e.g. abolishing intelligence agencies altogether) to retaining the status quo. Nothing was regarded as "off-the-table." The Commission did not approach its task as recommending change for the sake of change, however.

In the report that follows, the recommendations of the Commission are numbered and set out in bold type in each chapter. Key findings and conclusions are set out in bold italics.

At the request of the Commission, security experts from the Intelligence Community reviewed the report for security concerns immediately prior to printing but the substance of the Commission's findings and recommendations did not change as a result of this review.

Finally, the Commission prepared draft documents to implement its recommendations, which are being transmitted separately to the President and to the congressional intelligence committees.

CHAPTER 1: THE NEED TO MAINTAIN AN INTELLIGENCE CAPABILITY

THAT the United States should maintain an intelligence capability after the Cold War is not a matter in serious dispute. The world of the 21st century is likely to be as fraught with peril and uncertainty as the world left behind.

The United States finds itself in a predominant leadership role, whether sought or not, and the exercise of that leadership has become more complicated. New forces are at work and new dynamics at play. The Government must understand them in order to respond to them. Often the options available to it will depend upon how early problems are identified. Choosing the right option, in turn, will depend upon knowing what the consequences are apt to be. Once a course is chosen, it becomes important to know what the effects of the decision have been so that adjustments can be made if necessary. In every instance, making the right choice will hinge upon the quality of the information available.

The volume of information openly available to the Government in the media and over computer networks has exploded in recent years, a trend which will continue. Yet intelligence capabilities will continue to be needed to collect information that is not available through conventional means. Once such information is obtained, analytical capabilities will be needed to combine it with the rapidly proliferating information available from other sources and seek to produce an objective assessment free of policy predilections.

Where the process works, intelligence provides information and insights that are unique, reducing the uncertainty of decisionmaking at all levels—from the President to the infantry platoon leader wondering what lies over the next hill. With it, there is a better chance of avoiding crisis of war, of success on the battlefield, of reaching and enforcing international agreements, of investing in the right military capabilities, and of protecting U.S. interests at home and abroad.

There will inevitably be a considerable body of information bearing on matters such as these that is not available to the U.S. Government through conventional means. The reasons for this are apparent:

- Some governments will seek to deny access to their territory to the outside world.
- Countries that plan hostile actions against others will seldom announce their intentions in advance and will try too conceal their preparations.
- Most countries will not provide detailed public accountings of their military capabilities or their plans for developing such capabilities.
- Once military forces have been deployed against the U.S. or its allies, adversaries will attempt to conceal their plans and intentions as well as the size, composition, and disposition of their forces.
- Countries that violate international treaties, United Nations resolutions, or international norms of conduct will ordinarily conceal their actions.
- Governments involved in diplomatic negotiations with the U.S. will not ordinarily reveal their strategies and objectives.
- Illicit activities such as terrorism, drug trafficking, and espionage will be carried out in the shadows, not in the open.
- Environmental and humanitarian disasters will occur in places that are not readily accessible and require information beyond the ability of observers on the ground to collect.

There are limits to what intelligence can provide. Intelligence may be able to collect "secrets" (information that is knowable but hidden) but some information will necessarily remain "mysteries"—it simply cannot be known. What a foreign leader is thinking, for example, cannot be known unless the leader makes it known. Whether the same foreign leader will be in power in a year's time is a "mystery" only time will reveal.

The efforts of some countries to conceal their plans and activities will succeed despite the best efforts to learn of them. No matter how many collection capabilities U.S. intelligence deploys, relevant information will be missed. Human agents will not have access to what is needed. Technical systems will not be in the right place at the right time or will focus on the wrong target or will simply be thwarted by bad weather. Even if relevant information is physically acquired by technical systems, it may not be processed in a manner that permits analysts to identify or use it.

Analysis is subject to similar foibles. It may be based on intelligence that proves inaccurate or unreliable or fails to take into account all of the available information. It may address the wrong issue or reach the wrong conclusions or reach the policymaker too late to influence the decision at hand.

One should not expect perfection. Intelligence is simply a hedge against uninformed decisionmaking, and even the most sophisticated of collection systems and analytical talent cannot provide guarantees.

Compared with the rest of the world, the intelligence capabilities of the United States are immense. No other country devotes as many resources to this type of activity. Billions of dollars have gone into building sophisticated technical systems over the last 50 years, and billions more will be required to replace these systems as they are lost or worn out or become obsolete or ineffective. Substantial sums are also required simply to operate them and keep pace with developments in technology. For all but a few countries, the cost of mounting an intelligence capability on a scale approaching that of the United States is prohibitive. While a number of governments are exploring investments in expanded intelligence capabilities, the preeminence of the United States in this field is not likely to be challenged, if we choose to maintain our advantage.

Precisely because of this position of strength, however, some believe the United States can afford to cut back its intelligence capabilities, at least until the next war or crisis comes along. But these are not capabilities that, if abandoned or allowed to wither, can easily or quickly be resuscitated. Whether a satellite system or a human agent is involved, neither can be developed and deployed without a significant investment of effort and years of time. Both are dependent upon large and competent infrastructures, and such infrastructures cannot be maintained without a degree of permanence and commitment.

Others believe U.S. intelligence activities should be cut back or eliminated because they perceive their overall contribution to policymaking to have been marginal, even, at times, negative. When considered in terms of its substantial cost and the frequency with which it has been a source of political embarrassment to the United States, the advocates of this view conclude, intelligence is not worth the candle. Others question the competence of U.S. intelligence agencies—in particular, the CIA—to carry out their missions. While the Ames spy case demonstrated the CIA's inability to detect a relatively clumsy spy who compromised the core of its Soviet operations, it was but the worst in a series of operational failures experienced by the CIA and other intelligence agencies, most of which at one time or another have suffered severe losses due to spies in their midst. Others fault

intelligence agencies for "gold-plating" their facilities, wasting government funds, and keeping their overseers in the dark.

As noted in the Introduction, there have been problems, especially at the CIA, some of which have been substantial. While these episodes are deplorable, using them to justify cutting back or eliminating intelligence capabilities is a leap the Commission is unwilling to make. Problems are, to some degree, unavoidable where intelligence activities are concerned, despite the best of intentions or management structures. Operations will, on occasion, be compromised despite reasonable precautions being taken. Mistakes will occur either as a result of poor judgment or individual incompetence. This is not to excuse or minimize such failures, or to suggest that every reasonable effort should not be made to prevent them, but only recognize that problems to some extent are inevitable and, in the United States more so than in other countries, will continue to be highly publicized. The issue is whether the benefits justify the costs, including the problems which inevitably will occur.

For the public, this is particularly difficult to assess. Over the years, Americans have been exposed principally to the failures of intelligence and are largely oblivious of its successes. The Commission, on the other hand, has seen both. While failures have occurred too often, they have hardly been the norm. The accomplishments of U.S. intelligence have been, and continue to be, impressive. The details of specific cases cannot be made public without raising security concerns, but the following examples, *all occurring since the Cold War ended*, illustrate how U.S. intelligence serves the nation's interests:

- U.S. intelligence uncovered the first evidence suggesting that North Korea was planning to construct a nuclear weapons capability and supported the subsequent diplomatic efforts to restrain and end such activities.
- In at least two cases, with the help of U.S. intelligence, the sale of radioactive materials that could be used in the production of nuclear weapons was halted by other governments.
- Since 1990, U.S. intelligence has uncovered the clandestine efforts of several countries to acquire weapons of mass destruction and their related delivery systems. In some cases, this information provided the basis for diplomatic actions by the United States and by the United Nations to counter such efforts.
- U.S. intelligence played a crucial role in supporting U.S. combat operations in Panama and the Persian Gulf by collecting information on the size, capabilities and location of hostile forces, providing information which permitted the targeting of precision-guided weapons, assessing the damage inflicted by U.S. and allied aircraft, and warning of threats to the security of U.S. and allied forces.
- The deployment of U.S. military forces to Somalia, Rwanda, Haiti, and Bosnia to perform other than combat missions similarly received the vigorous support of intelligence agencies, which provided information on threats to the security of U.S. forces as well as on local conditions.
- U.S. intelligence played a key role in the rescue of the downed American pilot in Bosnia.
- U.S. intelligence provided support key to the U.S. side in numerous bilateral and multilateral negotiations.
- U.S. intelligence has played an instrumental role in the efforts of the Colombian government to break up the Cali drug cartel, including the arrest and/or capture of

its leaders, and, in other cases, provided information which kept drug shipments from reaching the United States.

- U.S. intelligence has played key roles in helping other countries identify and/or arrest several notorious terrorists, including Carlos the Jackal in Sudan, the alleged ringleader of the World Trade Center bombing in the Philippines, the head of the Shining Path terrorist group in Peru, and those involved in the bombing of Pan Am 103.
- On at least two occasions, U.S. intelligence provided information that led to successful U.S. diplomatic efforts to head off potential armed conflicts between two countries.
- Information was provided by U.S. intelligence on two occasions which foiled assassination plots abroad and led to the arrest of the perpetrators.
- In several instances, U.S. intelligence uncovered foreign competitors of U.S. commercial firms using bribery and other illegal tactics to obtain contracts with foreign governments. Diplomatic intervention with the government concerned to assure a "level playing field" eventually led to a U.S. firm obtaining the contract by winning the competition.
- U.S. intelligence has identified violations of military and trade sanctions imposed by the United Nations in connection with the situations in Iraq and Bosnia, and provided the principal capability for monitoring the "no-fly" zones in both countries.
- On several occasions, U.S. intelligence provided information warning of financial collapse in other countries, leading to actions by the United States and other governments.
- U.S. intelligence has provided information with respect to human rights abuses and election-rigging by certain governments which has altered the U.S. diplomatic posture towards those governments.
- U.S. intelligence has provided information about the military capabilities of other governments that has altered the research and development of U.S. weapons systems, providing potential cost savings and improving their effectiveness.
- U.S. intelligence has provided information to civil authorities in the United States, as well as in other countries, to help cope with natural disasters, environmental problems, and humanitarian crises.
- U.S. intelligence has supported United Nations' peacekeeping and other operations around the world.
- Considerable information has been provided by U.S. intelligence to the Bosnia War Crimes Tribunal.

It is impossible to quantify the accomplishments of U.S. intelligence of which these are examples. Clearly, however, over the last five years conflicts have been avoided, wars shortened, agreements reached, costs reduced, and lives saved as a result of the information produced by U.S. intelligence.

The United States had such information only because it chose to maintain a dedicated and capable intelligence apparatus. While that apparatus is expensive and will from time to time be a source of embarrassment, even consternation, the Commission has no difficulty reaching the conclusion that it is justified. Intelligence is an important element of national strength. The country should not lose sight of this amid the spy scandals and management failures of recent years. The performance of intelligence can be improved. It can be made more efficient. But it must be preserved.

CHAPTER 2: THE ROLE OF INTELLIGENCE

WITH the end of the Cold War and the reduced need to focus on the former Soviet Union, many observers believed that the Intelligence Community was looking for new missions to justify its existence. The Commission found, to the contrary, that the core missions of U.S. intelligence have remained relatively constant. There has been a substantial shift in intelligence requirements and priorities away from Cold War targets, but the missions intelligence agencies are expected to perform have not changed dramatically with the end of the Cold War.

This is not to suggest that the functions and missions of intelligence should not, or will not, change. Each administration should set the guidelines for intelligence activities and, within these guidelines, establish in a timely fashion specific requirements and priorities for the conduct of those activities. These will fluctuate according to the world situation, the availability of resources, and the needs of the Government. Such fluctuations make it essential that senior policymakers devote frequent, if not constant, attention to updating the priorities and collection capabilities that will ensure that the United States retains a strong national security posture. (Chapter 3 discusses how such a process might work.)

This chapter outlines the key functions of intelligence and concludes with a list of what the Commission sees as appropriate missions for U.S. intelligence as the country enters the 21st century.

THE FUNCTIONS OF INTELLIGENCE

U.S. intelligence has two broad functions—collection and analysis—and one relatively narrow one, covert action. An additional function—counterintelligence—is integral to the entire intelligence process. While the need for collection and analysis is generally understood and accepted, there is less acceptance of covert action as an appropriate intelligence function and less understanding of the critical importance of counterintelligence.

COLLECTION

Collection, as a function of intelligence, appears straightforward, and its necessity is not seriously challenged. Through various means, intelligence agencies collect information about foreign persons, places, events, and activities that is needed by the U.S. Government but cannot be (or is not easily) obtained through publicly available sources or diplomatic contacts.

In practice, however, this role involves numerous complexities. For example, intelligence analysts need publicly available information to perform analysis, identify gaps in their knowledge, and to task intelligence collectors. Do intelligence agencies "collect" publicly available information as well? Do intelligence agencies attempt to collect information to meet the needs of *any* Government official? Does anyone confirm that the need exists, i.e. that the information is not otherwise available to the Government, or that the need, if it does exist, justifies using expensive and/or risky intelligence capabilities to obtain it? What if intelligence officials know in advance that what they can collect will be of marginal value compared to what can be obtained from public sources? Do they still attempt to collect it? What if the information being sought pertains to a friendly or allied foreign government? Do intelligence agencies undertake collection activities regardless of their potential political cost?

Intelligence managers in each of the principal collection disciplines—signals intelligence (SIGINT), imagery intelligence (IMINT) and human intelligence (HUMINT)—confront such questions daily. To address these issues, elaborate collection management systems exist for each of the disciplines that establish validated requirements and priorities (further described in Chapter 3). Together, intelligence professionals and representatives from the policy agencies attempt to weigh competing requirements, assess the availability of relevant open source material, and address the issues raised by the questions above.

The Commission believes that intelligence collection systems, technical or human, normally should not be used for the purpose of collecting publicly available information, although publicly available information will often be collected as a collateral byproduct in the course of intelligence-gathering. To the extent that publicly available information is needed to support intelligence analysis and collection, it should ordinarily be obtained by intelligence agencies through other than clandestine means. Indeed, the collection of publicly available information should be considered a support function rather than a task for intelligence collection. There will be times, however, when information is "publicly" available but not readily accessible (for example, newspapers or radio broadcasts in North Korea or Iraq), and intelligence collection capabilities provide the only means to obtain it.

Intelligence collection capabilities, technical or human, also should be used only to collect information that can reasonably be determined, or that has been previously validated, to be of importance to a specific policymaker or intelligence user.

Finally, all intelligence collection must be weighed in terms of overall U.S. foreign policy interests. When collection activities are contemplated against allied or friendly governments, there should be a rigorous weighing of the political costs against the benefits. Senior policy officials must be involved in this process.

Analysis

The analytical function raises similar practical issues. In theory, intelligence analysts take information provided by perhaps all three collection disciplines, combine it with information from publicly available sources, and produce "all source" analysis for the customer. Because the analysis contains information obtained by intelligence sources, it is typically classified.

Because intelligence analysts have ready access to information from a wide range of publicly available sources, the question arises whether they should provide analysis based exclusively on such open sources if no significant intelligence is available on the subject. Also, if the analyst knows in advance that information obtained through intelligence will provide little of relevance to the overall analysis of a subject, should he or she nevertheless attempt to satisfy the request of a customer for an "all source" analysis? If an analyst accepts a request but finds the information produced by intelligence sources is marginal and the request can be satisfied by publicly available information, should he or she still produce an analytical assessment, or advise the customer to go elsewhere? If produced, should the assessment be classified simply because it was done by an intelligence agency? The Commission found that in practice, these issues are worked out on an *ad hoc* basis between analysts and their customers.

The Commission believes that intelligence agencies should not satisfy requests for analysis when such analysis could be readily accomplished using publicly available sources, unless for some reason the results of such analysis would require confidentiality or the specific expertise of the analyst would add significantly to the analysis of the open

source material. For example, a personality profile prepared on a friendly foreign leader might be taken entirely from public sources but nonetheless require confidential handling.

The Commission also believes that in general intelligence agencies should not accept requests for analysis when it is clear in advance that the information available from intelligence sources would have marginal impact on a particular analysis, unless there are special circumstances present that necessitate handling the request as an intelligence matter.[1]

COVERT ACTION

Covert actions (as distinguished from the covert *collection* of information) are used to *influence* political, military, or economic conditions or situations abroad, where it is intended that the role of the U.S. Government will not be apparent or acknowledged publicly. These might consist of propaganda activities, support to political or military factions within a particular country, technical and logistical assistance to other governments to deal with problems within their countries, or actions undertaken to disrupt illicit activities that threaten U.S. interests, e.g. terrorism or narcotics trafficking. Such actions complement and supplement parallel overt measures (e.g., diplomacy, trade sanctions, or military activities) undertaken by the Executive branch. By law, covert actions can be undertaken only in support of an "identifiable" foreign policy objective.

Responsibility for carrying out covert actions rests with the CIA, whose Director is charged by the National Security Act of 1947 to "perform such other functions and duties related to intelligence affecting the national security as the President or the National Security Council may direct." By Executive Order, CIA alone is specifically authorized to undertake covert actions that are individually authorized by the President, although other departments and agencies may also be directed to undertake or support covert actions as the President may authorize.

Since the end of the Cold War, the number and size of covert action programs have shrunk substantially, reflecting the extent to which they were prompted by the superpower struggle. Nonetheless, these programs continue to be undertaken to support ongoing policy needs.

The Commission addressed whether the United States should undertake covert action at all. Some witnesses expressed the view that there is no longer a need for covert action, and that, on balance, it has caused more problems for the United States than it has solved. The Government, they argue, has been frequently embarrassed by such operations and been criticized domestically and abroad as a result. Also, it is argued, covert actions comprise a minute part of the intelligence budget, but require a disproportionate share of management and oversight.

Most witnesses, however, including all of the former cabinet-level officials who addressed the subject, believed it essential for the President to maintain covert action as an option. Citing examples such as the need to disrupt the activities of a terrorist group, hamper the efforts of a rogue state to develop weapons of mass destruction, or prevent

[1] In Chapter 8, the Commission proposes the creation of a new, broadly based analytical entity in which intelligence analysts would participate, that would prepare unclassified assessments as well as assessments where the intelligence contribution is expected to be marginal. However, the preparation of such assessments is not envisioned as a function of intelligence analysis generally.

narcotics traffickers from manufacturing drugs for shipment into the United States, the proponents argue that the United States should maintain a capability short of military action to achieve its objectives when diplomacy alone cannot do the job.

In 1975, the Rockefeller Commission investigated alleged abuses in certain covert action programs and concluded that there were "many risks and dangers associated with covert action . . . but we must live in the world we find, not the world we might wish . . . [Therefore] covert action cannot be abandoned, but . . . should be employed only where clearly essential to vital U.S. purposes and then only after a careful process of high level review." ***This Commission strongly concurs with this conclusion. Moreover, the Commission notes that the laws governing covert actions do contemplate a "careful process of high level review," including approval by the President and notification to Congress.***[2]

This Commission believes that covert action must be consistent with specific U.S. foreign policy objectives in the targeted area. Covert actions should be undertaken only where there is a compelling reason why U.S. involvement cannot be disclosed. Further, the range of covert action options should be weighed to ensure that the methods employed are only as aggressive as needed to accomplish the objective(s). The costs of disclosure must be carefully assessed, and, where such costs are significant, the operation should be initiated only in the most compelling circumstances.

Some witnesses recommended that paramilitary covert actions—which typically involve arming, training and/or advising foreign forces—be conducted by the Department of Defense rather than the CIA. These individuals argued that the military is better equipped than the CIA to carry out such operations. Others argued that it is neither feasible nor desirable for U.S. military personnel to undertake such covert activities.

The Commission concludes that responsibility for paramilitary covert actions should remain with the CIA. CIA has extraordinary legal authorities and an existing infrastructure that permit the secure conduct of clandestine operations, whereas the military does not. Giving this function to the military would also involve it in a controversial role that would divert attention from other important responsibilities. The military should

[2] The legal framework for approval and reporting of covert action, originally enacted in 1974 by the Hughes Ryan Amendment to the Foreign Assistance Act of 1961, is now set forth in Sections 503 and 504 of the National Security Act of 1947 and 50 U.S.C. 413b and 414. These provisions prohibit any department or agency from expending any funds to engage in a covert action unless the President has signed a written "finding" determining that the covert action is "necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States." The President is required to ensure that the congressional intelligence committees are notified as soon as possible after a finding is signed, except if the President determines that "it is essential to limit access to a finding to meet extraordinary circumstances affecting vital interests of the United States, the finding may be reported only to the four leaders of the congressional intelligence committees and the four leaders of the House and Senate."

The established approval process includes a review of the proposed covert action by the Deputies Committee of the National Security Council (including senior policy representatives from the Departments of State, Defense, Justice, and Treasury, the Joint Chiefs of Staff, and the Office of Management and Budget, as well as the President's National Security Advisor) to ensure that the action is consistent with U.S. policy, is appropriate in scope for the situation, does not violate U.S. law and is properly funded. The covert action proposal is then submitted to the full NSC for approval and ultimately to the President for signature. Currently, ongoing covert actions are re-validated each year by the NSC to ensure that they remain necessary to the national security and are supportive of U.S. foreign policy objectives.

provide support to paramilitary covert actions as needed but should not be given responsibility for them.

With respect to any changes needed to improve the existing capability, the Commission notes only that covert action programs of the future are apt increasingly to involve technologies and skills that do not appear to exist within the current infrastructure. More attention should be given to these deficiencies.

COUNTERINTELLIGENCE

The counterintelligence function involves protecting the country, as well as intelligence agencies, from the activities of foreign intelligence services. The Federal Bureau of Investigation (FBI) has principal responsibility for countering the activities of foreign intelligence services within the United States in order to protect both classified U.S. Government information and proprietary information held by U.S. industry. The CIA is responsible for coordinating U.S. counterintelligence activities abroad. Each of the military departments also has a counterintelligence element that operates domestically and overseas.

Each of these elements has offensive and defensive missions. Offensively, they attempt to recruit agents within foreign intelligence services to ascertain what, if any, operations are being undertaken against the United States; they monitor the activities of known or suspected agents of foreign intelligence services; and they undertake operations to ascertain the targets and *modus operandi* of foreign intelligence services. Defensively, they investigate cases of suspected espionage and prepare analyses for government and industry concerning the foreign intelligence threat. The FBI has principal jurisdiction to investigate suspected espionage within the United States, although all intelligence agencies maintain internal capabilities to undertake preliminary inquiries of their own employees. Military counterintelligence elements have concurrent jurisdiction to carry out counterintelligence investigations of their respective military personnel.

Counterintelligence, as a function of intelligence agencies, however, goes much beyond detecting and monitoring the activities of foreign intelligence services and investigating employees suspected of espionage. Counterintelligence is an integral part of the entire intelligence process. All agencies that undertake intelligence collection, whether through human or technical means, must be constantly on guard that what they are collecting is genuine. This requires continuous evaluation of their sources as well as the information gathered from them. Intelligence analysts who are familiar with the totality of information on a particular topic are often in a position to detect anomalies.

Historically, intelligence agencies have not performed this crucial function very well. Virtually all have suffered severe losses due to a failure to recognize anomalous behavior on the part of their own employees. Some have also had problems recognizing anomalies in the behavior of their sources or in the appearance or actions of their targets. The Ames spy case revealed serious shortcomings in both categories.

In the wake of the Ames case, the Intelligence Community made sweeping changes to its counterintelligence infrastructure. A new policy board, reporting to the Assistant to the President for National Security Affairs, was established to coordinate counterintelligence activities and resolve interagency disagreements, and a "national counterintelligence center" was created to share and evaluate information regarding foreign intelligence threats. In addition, the CIA made numerous improvements to its counterintelligence and security posture. (CIA's actions are discussed further in Chapter 6.)

Perhaps more than any other function of intelligence, counterintelligence has undergone the most significant change over the last two years. The question is whether these changes will have a long-term positive effect. The Commission believes it is still too early to evaluate this issue.

Because counterintelligence is so crucial to the success of the entire enterprise, however, the Intelligence Community must sustain the renewed emphasis recently placed on this function. Counterintelligence must be viewed not as an annoying intrusion but rather as an integral part of the intelligence process. It must focus not only on protecting our own sensitive information, but equally on efforts to manipulate our collection and analysis, through double agents or other means. This requires a certain openness of mind and a willingness continually to balance the conclusions drawn from intelligence with the possibility of deliberate deception by a target.

THE MISSIONS OF INTELLIGENCE

In this section, the Commission identifies what it believes are necessary and appropriate missions for the Intelligence Community as it enters the 21st century. Many are traditional missions that require little explanation. A few, however, raise issues needing elaboration.

Support to American Diplomacy

The United States emerged from the Cold War as the world's only multidimensional (e.g. military, economic, and political) "superpower." It will have global commitments and global interests for the foreseeable future. Supporting American diplomats and foreign policy decisionmakers will continue to be a principal mission for U.S. intelligence.

This support entails providing advance warning of developments in other countries that will or could affect U.S. interests. Such advance warnings give U.S. policymakers the time to frame an appropriate response and, if possible, to avoid conflicts that might require the introduction of U.S. forces.

Intelligence can also provide information that assists policymakers in determining which of several diplomatic steps may be most effective. Ideally, the best intelligence is precisely that information that provides U.S. policymakers with the leverage to achieve U.S. objectives in international affairs without the commitment of U.S. forces. Intelligence also provides information that serves as the basis for U.S. diplomatic initiatives in bilateral and multilateral treaty negotiations.

Support to Monitoring of Treaties and Other Agreements

Intelligence is also essential for monitoring the multitude of treaties, agreements, and sanctions to which the U.S. is a party or has an interest, for example, the dismantlement of the nuclear arsenal of the former Soviet Union, economic sanctions against Iraq and other countries, and agreements prohibiting the proliferation of weapons of mass destruction.

Support to Military Operations

Another traditional mission of the Intelligence Community is to provide support to U.S. military operations. This mission encompasses not only warning of attack on U.S.

territory and installations, but also providing information needed to plan for and carry out military operations of all kinds. In the past, this has largely involved the provision of order of battle information on opposing military forces: their size, nature, location, morale and capabilities. In recent years, however, this mission has been rapidly expanding.

U.S. military operations since the Cold War have been carried out largely in the context of multilateral commitments of forces, increasing the need for joint planning and execution. Ironically, the number of occasions where U.S. military forces have been deployed outside the United States since the Cold War has greatly exceeded the rate of such deployments during the Cold War. Moreover, neither the location of such deployments, e.g. Panama, Somalia, Rwanda, Haiti, nor their purposes, e.g. preventing famine or genocide, "nation building," emergency evacuations, were typical of the Cold War period.

Recent years have also seen radical change in the nature of warfare. The 1991 Persian Gulf war lasted only a few weeks, but signaled a quantum leap in U.S. military capability. The world saw U.S. weapons fired from aircraft, ships, and land batteries far from the point of impact and delivered with pinpoint precision and devastating consequences. The war ended quickly, and U.S. casualties were minimal.

To a large degree, American success in the Persian Gulf war was due to information provided by intelligence systems both at the national and tactical levels. While achieving timely dissemination of such information was not without its problems, never before had so much information been gathered and relayed to a combat force so rapidly with such effect. The military began to look even more seriously at how intelligence capabilities could be brought to bear on their problems.

The Commission notes that the President recently issued a directive making support to military operations the highest priority for U.S. intelligence agencies. ***While the Commission agrees that the protection of U.S. lives is paramount and that the support of U.S. forces in, or with the prospect of, combat, is of the highest priority, we believe it equally important, to this end, to have intelligence that allows the United States to achieve its goals and yet avoid the commitment of military forces, whether that is accomplished through diplomatic action or other means.***

Support to Defense Planning

U.S. intelligence should also continue to support defense planning, another traditional mission. This mission entails providing information on foreign military capabilities in order for defense planners to shape the size, nature, and disposition of U.S. military forces. It also includes necessary information to guide military research and development activities and future military acquisition decisions. It encompasses information about foreign military tactics and capabilities, which can then be used to train and protect U.S. forces.

Economic Intelligence

The Intelligence Community has collected and analyzed economic information for close to fifty years. This activity focused on those areas that could affect U.S. national interests, including the economies of foreign countries, worldwide economic trends, and information to support trade negotiations. While much of this information was available from public sources, there were many countries where such information was restricted or not readily available. Intelligence filled a considerable void.

Now, after the Cold War, far more economic information is openly available, causing some to urge that the Intelligence Community abandon or cut back its historical role in economic intelligence, particularly macroeconomic collection and analysis. Some recipients of this analysis complain that it adds little to what they already know. Intelligence analysts concede that approximately 95 percent of the analysis on economic topics now comes from open sources. Policymakers have access to these sources and often have more sophisticated analytical capabilities at their disposal than does the Intelligence Community. Clearly, if the policymaker can satisfy his or her needs from these sources, he or she should do so.

On the other hand, there remains the five percent added by intelligence. Reliable information about economic conditions in certain countries continues to be unavailable. In these cases, accurate information could be crucial to decisionmaking. In some contexts, policy agencies may need to rely on intelligence agencies to perform economic analysis to preserve confidentiality even if open sources form the principal basis of such analysis, for example, in supporting trade negotiations.

The Commission believes that the collection and analysis of economic intelligence are missions that require particularly close coordination between producers and consumers in order to ensure that the intelligence contribution adds analytical value. While the Commission believes the overall mission remains valid, it may be possible to decrease the level of effort in this area by relying more heavily on open source analysis produced by academia or the commercial sector.

At the same time, the United States and other countries have taken more aggressive steps to promote their commercial interests abroad, both to increase domestic prosperity and to strengthen their national security. The fear of becoming commercially disadvantaged and the desire to "level the playing field" have motivated a surge of multilateral and bilateral trade agreements in recent years. In the United States, the issue of economic competition has also focused attention upon the proper role of intelligence in promoting U.S. commercial interests abroad.

While other countries have used their intelligence services to spy on U.S. and foreign businesses for the benefit of their national industries, U.S. intelligence agencies are not tasked to engage in "industrial espionage," i.e. obtaining trade secrets for the benefit of a U.S. company or companies.

Increasingly, however, the intelligence Community has become involved in identifying situations abroad where U.S. commercial firms are being placed at a competitive disadvantage as a result of unscrupulous actions, e.g. bribery and "kickbacks," undertaken by their foreign competitors. When intelligence agencies discover such cases, they advise the Departments of State and Commerce, whose officers may then choose to take diplomatic action with the government concerned to correct the situation. The Commission was advised that on the basis of such diplomatic actions over the last three years, American firms had obtained billions in foreign contracts they would otherwise have lost.

Several friendly foreign governments have questioned this practice, suggesting that using U.S. intelligence services in this manner was inappropriate and could damage the bilateral relationship. Presumably, these governments had in mind cases where their own commercial firms might be involved in "tilting the playing field."

The Commission strongly agrees with the current policy and practice prohibiting intelligence agencies from clandestinely collecting proprietary information of foreign commercial firms to benefit private firms in the United States. The role of the

Intelligence Community is to provide support to the Government, not to the private sector. However, where intelligence agencies obtain information that U.S. commercial firms, through unfair trade practices such as bribery or "kickbacks," are being placed at a disadvantage in obtaining a contract with a foreign government, or where a foreign government is otherwise involved in the transaction, the Commission believes intelligence agencies should continue to report such information to the Departments of State and Commerce. These departments would be responsible for determining whether and how the intelligence information is used, taking into account, among other things, its effect on the bilateral relationship concerned.

Countering Activities Abroad That Threaten U.S. Interests

For the last ten years, U.S. intelligence has been particularly active in collecting and analyzing information to counter certain "transnational activities" that threaten the lives of U.S. citizens, U.S. installations abroad, and U.S. national interests. These newer missions include:

- **Counterterrorism.** Intelligence efforts focus on identifying threats to the United States and its citizens and facilities abroad, but also frequently provide warning to other countries of terrorist activities within their territory.
- **Counternarcotics.** Intelligence seeks to provide information to U.S. drug enforcement authorities to prevent drug shipments from reaching the United States and to assist other governments in shutting down production in countries where illegal drugs destined for the United States are produced.
- **Counterproliferation.** Intelligence agencies provide information on at least 20 nations that have developed, or may be developing, weapons of mass destruction, and/or ballistic missile systems to deliver such weapons. Some of these nations have a record of hostile intent towards the United States. Intelligence agencies attempt to identify efforts by other countries to build or acquire such weapons and/or their delivery systems where they violate international law or threaten U.S. interests. On occasion, intelligence agencies participate in actions to prevent such activities from taking place.
- **Countering International Organized Crime.** Intelligence focuses upon international organized crime principally as a threat to U.S. domestic interests, attempting to identify efforts to smuggle aliens into the United States, counterfeit U.S. currency, perpetrate fraud on U.S. financial institutions, or violate U.S. intellectual property laws. It also attempts to assess international organized crime in terms of its influence upon the political systems of the countries where it operates.

In all of these cases, intelligence information has provided the basis for U.S. diplomatic initiatives, supported U.S. law enforcement efforts to prevent and prosecute such activities, served as the basis for military responses in some cases, and has often been key to the efforts of other governments to bring such activities under control. Frequently, intelligence agencies provide assistance to other governments beyond mere information, for example, by providing training or specialized equipment to cope with certain threats. On occasion, intelligence agencies are authorized to undertake covert operations to counter them.

The Commission believes that each of these missions continues to be valid and, indeed, will become more important as these activities increasingly threaten our national security. (We discuss ways to improve the U.S. Government's overall efforts to combat these activities in Chapter 4.)

Of all these, only the counternarcotics mission raised any significant controversy during the course of the Commission's inquiry. While the Intelligence Community has technical collection capabilities that are not duplicated in the drug enforcement community, the Drug Enforcement Administration has responsibility, in coordination with host governments around the world, for investigating narcotics trafficking and preventing drug shipments from reaching the United States. Some witnesses contend that human source collection by the CIA essentially duplicates this mission, increasing the possibility of conflict as well as the possibility that the CIA will become tainted by sources involved in drug trafficking activities. While acknowledging that human source collection in the narcotics area does raise particular problems, ***the Commission is persuaded that CIA provides special expertise and focus in the counternarcotics area and should continue to perform this mission. CIA should continue to coordinate closely with the Drug Enforcement Administration and other federal departments involved in counternarcotics activities abroad.***

It is clear that there are limits to what the Intelligence Community can do in terms of its overall impact on the narcotics problem faced by the United States. On the other hand, the Government should use all of the resources at its disposal to cope with it. Intelligence agencies do provide unique information in support of U.S. drug enforcement efforts. ***The Commission believes these efforts should continue.***

Support to Criminal Justice and Regulatory Agencies

In addition to providing information to law enforcement agencies about terrorism, drug trafficking, international organized crime, and weapons proliferation, intelligence agencies also frequently are asked to collect or provide information they may have regarding foreign persons or entities who are the subject of criminal investigations within the United States. Intelligence agencies also respond to requests from a variety of U.S. regulatory agencies for intelligence information they may have pertaining to foreign persons or entities who are subject to regulation under U.S. law, for example, foreign banks that apply for a license to operate within the United States or foreign individuals seeking a visa to enter the United States.

Responding to these requests ordinarily requires only a fraction of intelligence effort or resources. It does, however, raise concerns about the protection of intelligence sources and methods, and, given the voluminous information that is ordinarily developed by, or available to, criminal justice or regulatory agencies, the search of intelligence records may yield little of value. Moreover, regulatory agencies often have difficulty using classified intelligence information because their actions must be based on a public record. ***While the Commission believes as a general proposition that intelligence agencies should continue to respond to these kinds of requests, a thorough assessment of the value likely to be added by intelligence should be made before such efforts are undertaken and given priority over other responsibilities.***

Collecting and Analyzing Environmental Information

The unique collection capabilities of the Intelligence Community are occasionally put to use to obtain information on threats to the world's environment, such as the dumping by the Soviets of radioactive substances in the Arctic or the nuclear meltdown at Chernobyl. Environmental hazards can directly threaten the security of the United States and its citizens, and environmental conditions in other countries can have an indirect effect by causing regional conflicts over scarce resources, uprooting foreign populations, and destabilizing foreign governments. The Community also monitors international compliance with environmental treaties, and provides information and imagery to cope with natural disasters both within the United States and abroad. Analysis of this environmental information is performed on a limited basis.

Over the years the Community's satellite programs have amassed a unique historical collection of ecological data and offer an impressive future capability for environmental monitoring. Scientists reviewing this material under a current Administration program have concluded that the data holds enormous potential for the precise measurement of deforestation, global-warming trends, and other important environmental matters. The President has signed an Executive Order authorizing the release of this type of historical information from the 1960–1972 period to scientists for study.

The Commission believes the use of technical capabilities to collect information on environmental problems is legitimate but should not duplicate what civil authorities are able to obtain. The priority given such collection should be weighed against other requirements. To the extent possible, information obtained by such collection should be made available to civil authorities in unclassified form. The Commission also sees a legitimate, though limited, role for intelligence analysis in this area. Civil agencies are ordinarily in a better position to analyze information relating to environmental matters, but there may be circumstances where involvement by intelligence agencies is desirable, for example, if they possess special analytical expertise in a given area.

Collecting and Analyzing Information on World Health Problems

Information on world health problems and the capabilities of foreign countries to cope with them has become increasingly relevant to the ability of the United States to predict and respond to crises in other countries and to protect the health and safety of U.S. military forces and humanitarian workers who may be sent to assist. The movement of dangerous diseases to the United States is another major concern, and health problems can pose threats to the stability of foreign governments.

In many cases, information concerning these problems can be obtained without resorting to the use of intelligence capabilities, but in other cases such information will not be readily available. ***The Commission sees a legitimate role for intelligence here, albeit one that does not involve substantial resources.***

Information Warfare

"Information warfare" refers to activities undertaken by governments, groups, or individuals to gain electronic access to information systems in other countries either for the purpose of obtaining the data in such systems, manipulating or fabricating the data, or perhaps even bringing the systems down, as well as activities undertaken to protect against

such activities. U.S. intelligence agencies have been involved in aspects of information warfare, both offensive and defensive, for many years. New impetus has recently been given to these roles, however, by the explosion in information systems and information systems technology.

Government and public communications, transportation, financial, energy, and other industrial systems have become critically dependent on a complex set of interconnected automated information and control systems. Many of these systems are potentially vulnerable to computer-based disruption, manipulation, or corruption by hostile individuals, groups, or countries.

A number of witnesses pointed to the lack of an effective governmental structure to coordinate efforts to protect computer networks in the public and private sector from electronic attack. While several such efforts are underway, many believe they are not fully coordinated and do not sufficiently involve the private sector. While these concerns may be justified, the scope of the actions required to deal with the problem, especially the protection of computer networks in the private sector, would necessarily exceed the roles and capabilities of U.S. intelligence agencies.

Collecting information about "information warfare" threats posed by other countries or by non-governmental groups to U.S. systems is, however, a legitimate mission for the Intelligence Community. Indeed, it is a mission that has grown and will become increasingly important. It also is a mission which the Commission believes requires better definition. While a great deal of activity is apparent, it does not appear well coordinated or responsive to an overall strategy.

CHAPTER 3: THE NEED FOR POLICY GUIDANCE

INTELLIGENCE agencies cannot operate in a vacuum. Like any other service organization, intelligence agencies must have guidance from the people they serve. They exist as a tool of government to gather and assess information, and if they do not receive direction, chances are greater that resources will be misdirected and wasted. Intelligence agencies need to know what information to collect and when it is needed. They need to know if their products are useful and how they might be improved to better serve policymakers. Guidance must come from the top. Policymaker direction should be both the foundation and the catalyst for the work of the Intelligence Community.

The drafters of the National Security Act of 1947 understood the importance of such guidance in creating the National Security Council (NSC).[1] The NSC was created to coordinate the policies and functions of the departments and agencies of the Government relating to all aspects of national security, including the intelligence function.

Since then, each Administration has created its own structure and procedures to meet the policy objectives and management styles of the President and his senior advisers responsible for national security. Historically, intelligence information has made significant contributions to the substantive work of the NSC, whatever its structure; but where top-level guidance for intelligence requirements and policies is concerned, the role of the NSC and its staff has varied.

In some Administrations, formal NSC committees composed of cabinet-level officials have been established to provide guidance on intelligence matters. Such committees have been supported by a small professional staff within the NSC. In other Administrations, the national security advisor has delegated most intelligence issues to a senior member of the NSC staff. In some Administrations, the NSC principals and/or staff have taken an active and consequential role in providing guidance on intelligence matters; in others, they have served principally to coordinate the intelligence response during times of crises.

INTELLIGENCE AS AN NSC FUNCTION FROM THE NIXON ADMINISTRATION TO THE PRESENT

President Richard M. Nixon took office in 1969 and created an NSC structure shortly thereafter. Not until 1971, however, did his Administration create an "Intelligence Committee," one of the four top committees within the NSC responsible for providing policy guidance on national security issues. In addition, the NSC structure during the

[1] The statutory members of the NSC are the President, the Vice President, the Secretary of State, and the Secretary of Defense. Secretaries and Deputy Secretaries of other Executive departments may also serve on the NSC at the pleasure of the President. The present NSC includes the Secretary of the Treasury, the U.S. Ambassador to the United Nations, the U.S. Trade Representative, the Assistant to the President for National Security Affairs, the Assistant to the President for Economic Policy, and the Chief of Staff to the President.

The Chairman of the Joint Chiefs is principal military adviser to the NSC and may attend and participate in NSC meetings. The Director of Central Intelligence also may attend and participate.

The NSC is served by a staff headed by the Assistant to the President for National Security Affairs (who is often referred to as the National Security Advisor). The composition and organization of the NSC staff are left to the discretion of the President.

Nixon Administration contained a separate committee to approve and coordinate covert actions (the 40 Committee).

In 1975, the blue-ribbon "Commission on the Organization of the Government For the Conduct of Foreign Policy" (the Murphy Commission) reviewed this structure and found it largely ineffective. The Murphy Commission recommended that the NSC Intelligence Committee "should be actively used as the principal forum for the resolution, short of the President, of the differing perspectives of intelligence consumers and producers, and should meet frequently for that purpose."

In 1976, almost two years into his presidency, President Gerald R. Ford issued a new Executive Order on intelligence, abolishing the existing NSC structure on intelligence and creating in its place a "Committee on Foreign Intelligence" (CFI). This new Committee was composed of the Director of Central Intelligence, the Deputy Secretary of Defense for Intelligence, and the Deputy Assistant to the President for National Security Affairs. The Administration directed this committee to "control budget preparation and resource allocation" for national intelligence, as well as to establish priorities for collection and production. The Executive Order spelled out several specific tasks the CFI should accomplish, among them giving direction on the relationship between tactical and national intelligence and providing "continuing guidance to the Intelligence Community in order to ensure compliance with policy direction of the NSC."

This structure proved short-lived. President Ford remained in office less than a year thereafter, and his successor, President Jimmy Carter, immediately replaced the existing NSC apparatus with a two-committee structure consisting of a Policy Review Committee (PRC) and a Special Coordinating Committee (SCC). Depending upon the subject matter under consideration, the PRC would be chaired by, and composed of, different Administration officials, including the DCI when it addressed intelligence issues. The SCC was chaired by the National Security Advisor, and addressed the review and policy considerations of special activities, including covert action.

In 1978, President Carter provided more specific guidance on intelligence matters and issued a separate Executive Order on intelligence. It stipulated that the PRC, when dealing with intelligence matters, would be responsible for the establishment of requirements and priorities for national foreign intelligence, review of the intelligence budget, and the periodic review and evaluation of intelligence products. It was also charged with submitting an annual report on its activities to the NSC.

Three years later when he assumed office, President Ronald Reagan abolished the Carter NSC structure without creating a separate standing committee on intelligence, relying instead on a separate element on the NSC staff. He also signed Executive Order 12333, a broad statement of intelligence responsibilities and policies, which provided that the NSC "shall act as the highest Executive Branch entity that provides review of, guidance for, and direction to the conduct of all national foreign intelligence, counterintelligence, and special activities, and attendant policies and programs."

Later, as part of a reorganization of the NSC staff, a series of "Senior Interagency Groups" (SIGs) were created, one of which dealt with intelligence. Chaired by the DCI, the "SIG-I" was chartered to establish requirements and priorities for national foreign intelligence, review the program and budget for national intelligence as well as proposals for sensitive operations.

In 1989, President George Bush eliminated the Reagan NSC structure, and returned to a two-Committee structure, consisting of a "Principals Committee" and a "Deputies

Committee." The Principals Committee was chaired by the National Security Advisor; the Deputies Committee, by his Deputy. A separate staff office coordinated intelligence programs.

Two years into the Administration, the NSC conducted the first in-depth review of intelligence requirements. The document that instituted the review, known as "National Security Review-29," noted that "senior policy makers traditionally have neglected their critical role in setting intelligence priorities and requirements." It produced a lengthy list of government-wide intelligence requirements, but it failed to assign priorities in a way that usefully guided collection efforts or the allocation of resources.

In 1993, President Bill Clinton took office. He retained the "Principals Committee/ Deputies Committee" structure to coordinate major foreign policy issues and created a system of "Interagency Working Groups" to handle more routine issues. A separate staff office coordinated intelligence activities. In April, 1995, a new presidential directive was issued which, for the first time, stated in priority order what a President considered to be his intelligence requirements and established a working group of mid-level policy officials to review more regularly intelligence policies and requirements.

Shortcomings of the Past

The Commission sees several shortcomings in the historical process described above. The institutional role played by the NSC in providing guidance and direction for intelligence activities has varied widely. Often substantial lapses occur at the change of Administrations when there is no guidance at all. As a result, a consistent level of guidance concerning appropriate roles for intelligence, as well as the guidance establishing requirements and priorities for collection and analysis, has, all too often, been missing.

In practice, the NSC's structures created to perform such functions often have foundered. Senior officials, such as cabinet secretaries or their deputies, who represent their respective departments and agencies at NSC-level meetings, usually have little or no background in intelligence and are inundated by the press of other duties. Intelligence is too often viewed as a support function that is "someone else's responsibility." Subordinates are increasingly sent to meetings in place of principals, and meetings become progressively less frequent. As a result, a true "consumer driven" intelligence process has never fully evolved within the NSC, regardless of the Administration in office.

The Commission believes the NSC as an institution should provide clearer guidance for intelligence, through regular tasking and a better organizational framework for handling intelligence issues. Several close allies visited by the Commission during its inquiry have effective mechanisms at the senior levels of governments to ensure that their intelligence agencies receive timely, ongoing guidance from the political level. In Great Britain, for example, a Cabinet-level office known as the Joint Intelligence Committee (JIC) brings together senior British policymakers and intelligence officials on a *weekly* basis. The JIC, functioning since 1936, is responsible for setting intelligence priorities on an ongoing basis, and for producing a weekly intelligence summary. Members include the principal producers and consumers of intelligence. While clearly the work and value of structures such as the JIC are facilitated where the government is considerably smaller than the U.S. Government and principally staffed by career civil servants, the Commission believes the concept embodied in the JIC can also be made to work in the United States.

What Needs to Be Done

The Commission recognizes that every President must be free to use and structure the National Security Council as he or she sees fit, including the performance of its statutory role to provide direction to the Intelligence Community. From the Commission's standpoint, however, the particular structure decided upon by a president is less important than a clear and consistent understanding and implementation of the roles it should perform. Even when Administrations change, the functions of the NSC should not. Top-level direction to intelligence agencies would be greatly strengthened by a more institutionalized role for the NSC, one that is not rewritten every two or four years. The more the role of the NSC varies, the more difficult it is to develop and sustain working relationships that provide clear, frequent direction for intelligence and guidance for its collection and analytic efforts.

In the view of the Commission, the institutional role played by the NSC structure should include setting the policy guidelines for intelligence activities, stating what the intelligence agencies are expected to do and what they should not do. The NSC structure should clarify, for example, whether intelligence agencies should collect economic intelligence or analyze intelligence on the environment, whether they perform analysis of publicly-available information, and what rules should govern intelligence-gathering where allied and friendly governments are concerned.

The institutional role of the NSC also should include providing guidance for ongoing intelligence collection and analysis, to say what is needed and when, clarifying what is helpful and not helpful. What are the issues on the "front burner" for the President and other policymakers? What information would fill a void? On what subjects is intelligence adding little of value? Where does intelligence have access to information that would be of considerable value, but is not being collected?

It should also be the institutional role of the NSC (but not the NSC staff by itself) to assess, from time to time, the performance of the Intelligence Community in satisfying their substantive needs as policymakers, reporting its conclusions, as appropriate, to the President.

In the section that follows, the Commission proposes a two-tier NSC structure for carrying out these roles. It is intended as a model for this and future Administrations.

Whatever NSC structure may be adopted for intelligence, however, it must not interfere with the direct reporting relationship between the President and the Director of Central Intelligence, which must be preserved. The importance to the intelligence function of having a strong relationship between the President and the DCI cannot be overemphasized. The Commission was consistently told by former DCIs that where their relationship was strong, it had repercussions across the entire Government, including the Congress, giving vitality and purpose to the whole enterprise. Conversely, where the relationship was weak, it took a heavy toll on the esprit and influence of the Intelligence Community.

3-1. The Commission recommends the establishment within the National Security Council of a "Committee on Foreign Intelligence" (CFI), chaired by the Assistant to the President for National Security Affairs and including the Director of Central Intelligence, the Deputy Secretary of State and the Deputy Secretary of Defense. The Chair should invite other senior officials to attend as may be appropriate given the meeting agenda.

The CFI should meet at least semi-annually and provide guidance to the DCI for the conduct of intelligence activities, to include establishing overall requirements and priorities for collection and analysis. Appropriate NSC staff should formulate the agendas and supporting materials for these meetings, with NSC members and their staffs providing such assistance as may be required. The CFI should report annually to the President on its activities.

3-2. The Commission recommends that a "Consumers Committee" be established as a subordinate element of the CFI. This Committee should be chaired by the Deputy Assistant to the President for National Security Affairs and should include senior representatives at the Undersecretary level of the parent CFI members as well as senior representatives of other principal intelligence producers and consumers within the Government, e.g. the Secretaries of Commerce and Treasury, the U.S. Trade Representative. The Consumers Committee should meet at least monthly and provide continuous, ongoing guidance with respect to the priorities for intelligence collection and analysis to meet the needs of the Government. The Consumers Committee should monitor and periodically report to the CFI with respect to how well the Intelligence Community is meeting the needs of consumers, identifying gaps and shortcomings where appropriate. The NSC staff should be responsible for formulating the agendas and supporting materials for each meeting, with NSC members and their staffs providing such assistance as may be required.

The Commission opted for this bifurcated approach for several reasons. The Commission believes that the major overarching issues in the intelligence area are best left to a small group, consisting of the principal cabinet officers who are responsible for, and the users of, intelligence. The Commission believes such a group should be chaired by the National Security Advisor because he can approach the issues from the viewpoint of the President and has responsibility for coordinating national security matters on his behalf.

However, it is unrealistic to expect such a senior group to play an active role in setting ongoing requirements and priorities for intelligence-gathering and analysis. This function necessarily requires more frequent meetings and must be carried out at a lower level of representation. Membership should be at a high enough level so that the participant can represent the policies of his or her agency or department, but also at a level where the participant can be a regular attendee at the monthly meetings. Whoever may be designated, however, should have or be able to obtain a grasp of the overall intelligence requirements and priorities of the department or agency they represent.

The Commission believes that a forum outside the Intelligence Community (but including a representative of the Intelligence Community) should evaluate the substantive contributions made by the intelligence agencies. Hence, this role is suggested for the Consumers Committee. This is a function that the NSC has not performed in the past but is needed for the effective operation of the Intelligence Community.

Finally, the Commission does not contemplate that either the CFI or its subordinate Consumers Committee would perform oversight or management functions. The DCI would continue to report to the President and not to either of these committees. The function of both bodies would be to provide guidance to the Director of Central Intelligence and, through him, to the Intelligence Community as a whole. If disagreements arose which could not be resolved inside the NSC structure, each cabinet-level official would retain the right to appeal to the President.

The President's Foreign Intelligence Advisory Board

While not a part of the NSC structure, the President has another body at his disposal to provide advice on intelligence matters—the President's Foreign Intelligence Advisory Board (PFIAB). First created by Executive Order in 1961, the PFIAB is charged with advising the President with respect to the quality, quantity, and adequacy of intelligence collection, analysis, counterintelligence, and other activities.[2] The PFIAB is also authorized to assess the adequacy of management, personnel and organizational arrangements in the intelligence agencies. Composed of private citizens, usually with some government experience, the number of PFIAB members has varied from one Administration to another.[3]

Historically, the PFIAB often has produced insightful and critical reports. Early boards were instrumental in analyzing and promoting the technical developments of the 1960s which revolutionized intelligence gathering. In the last several years, the PFIAB has looked at issues such as personnel practices within intelligence agencies and intelligence-sharing with multinational organizations.

The Commission supports the continuation of the PFIAB but believes that its role would be enhanced and its contributions more significant if it sought to perform functions that are not being performed elsewhere, either by the NSC or within the Intelligence Community itself. The Commission has noted in the course of its inquiry that very little thought is given by the Intelligence Community to the future, to finding creative technical or managerial solutions to the problems of intelligence or focusing on long-term issues and trends. By virtue of its membership, the PFIAB appears uniquely positioned to serve this function by bringing to bear the experience and expertise of the private sector and respected former government officials. Presidents must ensure that persons appointed to the Board have the qualifications necessary to perform this role and an adequate staff capability to support them.

[2] The PFIAB replaced an earlier "President's Board of Consultants on Foreign Intelligence Activities" that had been created by President Eisenhower in 1956. The PFIAB was disbanded in 1977 by President Carter but reconstituted by President Reagan in 1981.

[3] The current Executive Order governing the PFIAB, E.O. 12863 (Sept. 13, 1993), limits membership to 16 individuals.

APPENDIX H

A TALE OF COUNTERINTELLIGENCE*

A once sensational and mysterious intelligence betrayal is examined in the perspective of time for motivation and key circumstances.

THE DEFECTIONS OF DR. JOHN, BY DELMEGE TRIMBLE

Rain streaked the streets of Berlin, splashed on darkened houses, glistened in the light from and East-West border checkpoint. A sedan rolled up, its tires singing on the wet pavement. A customs guard sauntered out. For a moment there was only the throb of the engine, a murmur of conversation, the rhythmic click of the windshield wipers. Then the wave of a hand, and the car rolled across the Sandkrug Bridge into the darkness of East Berlin.

A simple incident on this warm, wet night of 20 July 1954, the decennial of a more famous 20 July. Simple, but so fraught with significance for Germany and the West that Chancellor Adenauer called it "terrifying." Dr. Otto John, president of the Office for the Protection of the Constitution, had defected. He was the most important Westerner fallen into Communist hands since the two British diplomats, Guy Burgess and Donald MacLean, had vanished from London in 1951, and far more important than they in point of implications for intelligence.

The puzzle was—and to some still is—the reason why, the causes behind the eastward flight of the Federal Republic's internal security chief in the company of a trumpet-playing gynecologist, a Dr. Wolfgang Wohlgemuth. The contemporary explanations ranged the spectrum. The easiest one, that Wohlgemuth was a Soviet agent who had

* Source: Delmege Trimble, "The Defections of Dr. John," *Studies in Intelligence*, 45th Anniversary Issue, Special Unclassified Edition, Central Intelligence Agency (Fall 2000), pp. 27–52.

drugged John and abducted him, foundered on facts that gradually came to light. Some said that John, a mixed-up idealist, had been spurred across the border by a misguided concept of political morality. Some regarded him as a victim of machinations on the part of the neo-Nazis and clerical and other reactionary circles around Chancellor Adenauer. His flight was pictured by others as that of a desperate man whose past was about to catch up with him. Yet others called him a long-time traitor and informer, even a secret Communist fanatic.

There were prejudicial grounds for some of the least pretty interpretations. John's weaknesses for alcohol and the opposite sex were well known, his favorite sport when pixilated being to snap the elastic of women's brassieres. It was persistently rumored that he was a double agent or a homosexual, and he certainly had an affinity for too many characters with one or both of these qualifications. Aside from his companion Wohlgemuth, who had connections with the East Berlin Charité Hospital and made no secret of his Communist sympathies, John was on good terms with Soviet agent Max Wonsig, blown at the Willi Kucher spy trial, and more notably with one Baron Wolfgang Gans Edler Herr von und zu Putlitz. Von und zu Putlitz had been a prewar British agent in the Nazi Foreign Office, whisked to the safety of England in 1938; subsequently he worked in the United States for OWI until he was fired and his valet had to support him by tending bar; later he returned to British employ in Germany; and in 1950 he started working for the Communists in East Berlin.

Yet the stereotype of the weak man made vulnerable by his lusts or corrupted by bad company is not one that fits the Otto John picture. And all the other theses, each arguable, strike only tangentially at the truth. Erich Ollenhauer may have come closer when he remarked, after John redefected and began to show increasing signs of a persecution and Messiah complex, "This is a case for the psychiatrists rather than the politicians." We cannot even now arrive at anything like a tidy analysis of the case, but we can achieve some understanding of it by tracing John's propensities during the Nazi and Nuremberg eras, reviewing the circumstances of his unlikely appointment and ineffectual tenure as president of the Bundesamt fuer Verfassungsschutz, and examining in detail his behavior just before and after his defection on that 1954 anniversary of the unsuccessful 20 July anti-Hitler coup.[1]

ROLE IN THE ANTI-NAZI UNDERGOUND

Otto John was born in 1909. Two friendships from his early life remained of importance in his adult career and were to play a part in the events of July 1954. During his school days at Wiesbaden in the mid-twenties he became a close chum of Wolfgang Hoefer, son of the school principal. The intensity of German schoolboy friendships is reflected in the eventual tragedy that flowered from this early acquaintance. Hoefer, whose mother was Jewish, emigrated to the United States in the late 1930's. He changed his name to Hoffer, became a U.S. citizen and a soldier. In 1945 he was sent to Germany and renewed his friendship with Otto John. In 1954, upon John's defection, he committed suicide.

An emotionally more important relationship for Otto was that with his brother Hans, another marked for tragedy. Hans, the younger, brighter, and sturdier, was the extrovert

[1] Except as otherwise indicated, the authority for factual statements in the following account rests in classified documents in U.S. intelligence files.

doer, Otto the troubled dreamer. Otto felt no fraternal jealousy; he adored the younger brother who, as long as he lived, supplied the balance Otto needed. Hans was to be tortured to death in the aftermath of the abortive July 1944 coup.

Otto studied for a career in the foreign service, mastering Spanish, French, and English. But when Hitler came to power membership in the Nazi Party became a prerequisite for aspirants to the foreign service, and he shifted to international law. Never a member of any political party (though after the war he once referred to himself as a quondam Socialist), he said his convictions were a blend of monarchism, old-fashioned liberalism, and anti-Nazism. He received the doctorate in law from Frankfurt University in 1935.

By 1936 both John brothers were in Berlin. Hans was studying law at Berlin University. Otto served for two years without pay at Tempelhof Airdome to qualify for final state law examinations in the service of Lufthansa. In 1937 he became assistant legal counsel, under Klaus Bonhoeffer, of the rapidly expanding civil airline. He was now in a position to do something positive about his anti-Nazi convictions. Through Klaus and his brother Dietrich, a Lutheran minister, he entered one of the circles that later were to band in the conspiracy against Hitler. An airline with routine flights into foreign countries was a convenient front for a conspiracy against a totalitarian regime.[2] Klaus Bonhoeffer assigned Otto to several courier runs.

When World War II broke in September 1939 Hans John went into the Luftwaffe as a lieutenant, but Otto remained with Lufthansa. That autumn he established connections with such anti-Nazis as the Social Democrat Wilhelm Leuschner and Col. General von Beck. Prince Louis Ferdinand, grandson of the Kaiser, had quit his job in a Ford plant in the United States to work for Lufthansa, and Otto John, along with Johannes Popitz, the Prussian Finance Minister, became a chief promoter of the Prince's pretensions to the throne in Carl Goerdeler's early schemes for a Hohenzollern restoration.[3] Louis Lochner, former chief of the Berlin Bureau of the Associated Press, said that on several occasions he accompanied John to meetings in Berlin of the Goerdeler and Louis Ferdinand groups.

Death was to sluff most of Otto's co-conspirators off the stage long before his own desertion, whether through natural causes, official executions, or the goon squads rampant at Germany's last gasp. But Louis Ferdinand remained a member of the cast through the last act. John cultivated him not only because he and his wife Kira, a former Grand Duchess of Russia, were very pleasant social companions but also because John, with his royalist inclinations, was flattered at being allowed to address the Prince by his intimate family nickname, "Lulu."

Beyond these contacts with conspiracy and his flights to neutral countries, Otto's specific resistance activities during this early period are unknown. In 1941 he passed considerable classified information about the Luftwaffe to U.S. correspondent Lochner. Strained attempts have been made to link him a little later with Rote Kapelle, the Communist radio-espionage group active in Berlin in 1941–42. No evidence is available to support any such connection, although it has been taken for granted that his brother Hans had Communist affiliations.

---

[2] Many clandestine interests capitalized on the advantages of this airline's international flights: Admiral Wilhelm Canaris' Abwehr faction, carrying its own intrigues against the Nazis, had planted agents in it; Himmler's SS and the Gestapo had both infiltrated it; and the Soviets are believed to have recruited a pilot on the Berlin-Moscow run, a man named Radunsk.

[3] Gerhard Ritter, *The German Resistance*, pp. 191–2.

When eyebrows were raised over the appearance of the healthy Otto in mufti, he entered the Abwehr, likely on Goerdeler's suggestion and through the good offices of General Oster, the activist conspirator under Admiral Canaris. He was assigned to Abwehrstelle Stettin but told that his primary mission was to seek better surrender terms for Germany once Hitler was removed, using his Abwehr commission simply as cover. Threads linking the various opposition groups were now being slowly knit, and John probably provided liaison among those in the Abwehr, in the Army High Command, around Leuschner and Julius Leber, Louis Ferdinand, etc., whose heretofore diffuse activity was manifest in the ineffectual half-dozen different attempts to remove Hitler between 1939 and 1943.

The year 1942 was eventful for him. He was using business trips to Madrid and Lisbon, ostensibly for the purpose of acquiring more Lufthansa runways, to re-establish resistance contacts with the British and try to activate the acquaintance between Prince Louis Ferdinand and President Roosevelt, who had once put the Prince up at Blair House. During this year he was turned in to the Gestapo by an aging and jealous pre-war mistress, Frau Ameliess Pabst, and was rescued by his Abwehr connections. Also in 1942 Hans returned from the Russian front badly wounded and was taken to the famous surgeon Dr. Sauerbruch, who numbered among his assistants at the Charité Hospital the fateful Wolfgang Wohlgemuth. Otto soon learned to know the comrade of his future eastward flight by his pet name, Wowo.

John's peace feelers were received with considerable suspicion by the Allies, especially since he was unwilling at this time to name any conspirators. On 20 February 1943 the British intelligence service issued from London a statement to the effect that the Abwehr or the Gestapo was possibly inspiring his activities as a deception. He persisted, however, using his intermediary Juan Terraza, one of the principal diplomatic secretaries in the Spanish Foreign Office and a close friend of Louis Ferdinand. His attentions were directed toward Graham of the British Embassy in Lisbon and Willard L. Beaulac of the American Embassy in Madrid. Beaulac, on instructions from Assistant Secretary of State Acheson, saw John at his home but made no commitments. He, too, was dubious of his sincerity.

John's sincerity as a representative of the military element of the resistance, a role he was soon to assume, is in fact questionable. He was a dissenter among dissenters, thoroughly disliking the generals and never believing they would act against Hitler. He considered the military component of the 20 July group very weak and continually warned against it.

As 1943 wore along, his approaches became more definite. In December he told his British contact in Madrid that he represented an internal opposition group consisting of industrialists, trade union leaders, churchmen, and generals, all strongly anti-Nazi and anti-USSR. He ticked off names and disclosed details of another plot to murder Hitler.[4] In February 1944 he again came to Madrid ostensibly on Abwehr business. This time he said he was remaining in Spain as a representative of the anti-Nazi generals. As cover he assumed the directorship of the sister Lufthansa company there.

He later told the British that he performed no Abwehr missions on his trips to Spain. In early June 1944, however, the British ascertained that he had transmitted information concerning Allied military intentions in Berlin. The nature of this information is not known;

[4] At about this time the report that John was a British agent being handled by Major F. Landsdale and Cmdr. A. Fuller of the British Embassy in Lisbon was conveyed from the Portuguese General Staff to a German Lt. Col. von Auenrode (alias Karschof), who in turn informed Admiral Canaris. Canaris, of course, took no action.

it was probably innocuous. In any case the British and American embassies in Madrid, for their part, got valuable data from him—on the results of Allied bombings of Berlin, the German V-bomb and its launching bases, and the experimental station at Peenemuende.

The current events leading to the ill-fated Generals' Coup was now quickening. Shortly after the Allied invasion of Normandy in June, John consulted in Madrid with Col. Georg Hansen, who as Canaris' successor at the head of the Abwehr was prospectively chief negotiator with the Allies, specifically General Eisenhower at SHAEF, once the revolt had succeeded. In early June he made arrangements that any message from the conspirators would be passed immediately from the American Embassy in Madrid to General Eisenhower. At the same time he learned, to the dismay of the conspirators, that the Western Allies would not consider negotiating a separate peace, and the British and Americans would probably make no effort to get to Berlin ahead of the Russians.[5]

There is conflicting evidence about his activities at the time of the attempted coup itself. According to his own story, he was called to Berlin to confirm in person his bad news of the unresponsiveness of the Western Allies, and arrived at Tempelhof Airdome on 19 July. He was at OKW Headquarters in the Bendlerstrasse on the afternoon of 20 July when Col. Klaus von Stauffendberg arrived from East Prussia to report that the bomb had gone off and Hitler could be assumed dead. He worked with the conspirators there until 9:30 that evening, when it became evident that this attempt on Hitler's life had also failed, pro-Nazi officers were regaining control, and conspirators were being summarily executed in the courtyard. The next morning, according to his account, Johannes Popitz' daughter told him of her father's arrest, and he went into hiding. He escaped to Madrid on 24 July by signing on as a mechanic on a Lufthansa manifest.[6]

John's story, however, is contradicted by the lists of applicants for Spanish visas and travel manifests from Aerodome del Prat del Llobregat. They show him arriving in Barcelona from Madrid via Lufthansa on 18 July and not departing for Berlin until 22 July. Allied intelligence regarded the variant embellishments of his account as probably fabrications and was inclined to suspect that Otto credited himself with activities rightly belonging to Hans. One MI-6 interrogator remarked that John seemed to change the story to keep from boring himself.

At any rate he turned up in late July or early August in Madrid, where he lived in a hotel some three weeks. On 25 August they smuggled him to Lisbon and hid him at a safehouse, the Boa Vista, which was also used by Spanish Communists. On 23 October the Portugese police raided this house and arrested John, the housekeeper Romero, and seven of the Spanish Communists.[7]

---

[5] Ritter, *op. cit.*, p. 282. The ultimate source is John himself.

[6] That John was one of the pathetically few rebels to escape has been cited to support a theory that he was a Gestapo agent infiltrated into the conspiracy. We have noted that he was out of sympathy with the generals, and he seems not to have been intimately associated with any resistance circle except Louis Ferdinand's; but the Gestapo theory is untenable. He would hardly have betrayed his beloved brother Hans. Moreover, two SS aids of Walter Schellenberg later testified that the Gestapo had partially penetrated the 20 July group, but not through Otto John.

[7] There are diverse accounts of this episode. One intelligence version has it that John was arrested because of his friendship for Professor Egaz Morriz, frequently referred to in Portugal as the unofficial Soviet ambassador. *Der Spiegel*, ten years later, said that he was arrested as a homosexual. Another section of the German press insisted that he was arrested at a fiesta when he got into a brawl over a woman.

John was jailed for several days at Caxias. Then the Portugese General Staff overrules the policy and turned him over to the British. He was flown to the UK on 3 November, accompanied by Cmdr. Fuller, his contact at the British Embassy in Lisbon.

IN THE BRITISH VICTOR'S SERVICE

On John's arrival in the UK there was a wartime snafu as to his identity, and he was interned as a high-ranking Nazi. According to his own story, Churchill at this time called him in for a consultation that last half the night. He was released from internment and transferred to the Political Intelligence Department of the Political Warfare Executive on 11 December. He was turned over to Sefton Delmer, a top reported for the London *Daily Express* and later for the *Times*, who was wartime director of the Morale Branch of PID. According to Delmer, John lived with him for 10 months. Delmer is another person who will reappear before this drama is acted out.

In 1945 and 1946 John worked for the British in various capacities—with PID on intelligence matters, on the POW reorientation program at Wilton Park, and on research for A tally of John's fellow-Germans—Dr. Honigmann, Eberhard Koebel, Karl von Schnitzler, and Putlitz, the agent-baron discharged by the OWI—is intriguing: all of them, like John, were later to decamp to the East Zone of Germany.

After the surrender in May 1945, John did not return to Germany with the bulk of the political exiles. He was working for the British War and Foreign Offices, interrogating German generals in the Kensington cage, and helping prepare legal documents for the approaching Nuremberg trials. At Nuremberg he worked as an adviser to the UK prosecution staff, a fact omitted in his own curriculum vitae.

Up to this time he could lay valid claim to being a German patriot. The cause which met catastrophe on 20 July had been a worthy one, that of revolt against the Nazis, not treason to the German nation. Its watchword was, "Against Hitler, for Germany." But when he returned for the Nuremberg trials, it was in effect as a German in British battle dress. He revisited with the wrath of a prosecutor the country which he had fled as a political persecutee. He kept aloof from other Germans working at the trials, attempted to conceal his identity and purpose, and spent his free time with his British colleagues, trying unsuccessfully to pose as an Englishman doing historical research in the documents of the Tribunal. The spirit of the trials themselves, in which righteous indignation at the Nazi horrors was not untainted by thirst for political vengeance, may have contributed further to the warping of John's character.

He was already showing psychoneurotic tendencies. In 1946 in London he attended a private War Office showing of a film on the Belzen concentration camp. Shortly after the movie, he told an intelligence officer five years later, the lower part of his face began to discharge a pus-like fluid and he suffered a species of nervous breakdown. His explanation was that the movie brought home to him the terrible failure of the 20 July revolt and all it stood for; he had been condemned to virtual inactivity since his flight to the UK and the accumulated frustration was simply too much for him. John clearly identified himself closely with the failure of the anti-Hitler resistance and had a strong guilt complex deriving probably from his brother's painful death. This reinforced his obsession with the July affair and his inability to compromise with anything remotely identifiable with Nazis, right-wing politicians, or German military traditions. His excessive drinking and other manifestations of emotional instability would be symptomatic of such a state of mind.

He may have had woman-trouble, too. In 1949, after practicing law in London for a year, he married Frau Lucy-Marleen Mankiewitz, the *mother* of the girl he had been expected to wed. His new wife, a German Jewess whose father was an old friend and adviser of Dr. Theodor Heuss, taught Wagnerian singing at Hampstead. She has been described as making up in charm and intellect for the greater beauty of her jilted daughter Gisela, with whom John had worked in a wartime British operation.

John's mistress, Frau Elsa Mueller Rudolph in Wiesbaden, the widow of a German pilot killed in action in 1943, was another who stood to be offended by this marriage. John wrote in explanation that he was marrying an older woman because of his need for balance, and moreover his bride had important political connections in the new Germany through her family. He hoped that he and Elsa could remain friends. They did. It was Elsa who, as nearly as can be ascertained, enlarged Otto's circle of acquaintances to include Ian Eland, who was later helpful in exposing and eliminating one of John's rivals for the presidency of the Verfassungsschutzamt.

In the fall of 1949, no longer trying to conceal his services to the UK, John became openly the chief German assistant to the British prosecution at the trial of General von Manstein in Hamburg. This time he apparently associated with the German lawyers defending Von Manstein. But he irked the defense, it is said, by deliberately twisting facts and evidence to the advantage of the prosecutors, many of whom relied heavily on him because of their unfamiliarity with the German language and with the organization and practices of the Nazi Reich. Several friends implored him at this time to get out of the business of delivering his countrymen to the Allied hangman, and their warning that he was alienating himself from his fatherhood must have increased his emotional stresses.

John was not doing awfully well financially in the UK. He was employed by the London solicitors James Brodie & Company on reparation and restitution cases, but he could not base a career on claims arising out of a past era. He suffered from the lack of the British citizenship that had been extended to Putlitz and certain other Germans. (At times he claimed that he had declined a proferred citizenship.) Germany, on the other hand, was getting back on her feet economically.

During 1949 and 1950 he made several trips to Germany to see friends in the Bonn government about a job. Jakob Kaiser, whom he had known as a leader of the Catholic trade union resistance, offered him one in his Ministry of All-German Affairs, but John declined on the ground that he deserved a higher rank than Ministerialrat. Foreign Affairs had no place for him because, he suspected, of his "anti-German" activities in the UK and his role at the trials. He also tried unsuccessfully for an appointment on the German delegation to the International Ruhr Authority.

THE PROTECTOR OF THE CONSTITUTION

In 1950 West Germany was passing through the interim stage on the road from occupation to sovereignty, and an important question was that of preserving ideological rectitude in the new state. The French did not want it to have any political police. The British favored an adaptation of Scotland Yard. The United States came up with an emasculated FBI plan. The Germans wanted to return to the pre-Hitler scheme, incorporating the political as Branch 1A into the national police. The eventual compromise was the watery conception of an Office for the Protection of the Constitution, a police force with no power to arrest. It was supposed to be a silent security service keeping tabs on the lunatic fringes to the right and left.

How was it that Otto John, a man who already showed signs of needing watching himself, almost an expatriate, whom Chancellor Adenauer is said to have disliked from first sight, was named head of the sensitive Bundesamt fuer Verfassungsschutz? Or, as the Germans put it in their rough peasant proverb, "Who put the goat in charge of the garden?" As assets he had an influential friend in Jakob Kaiser, his connections by marriage with President Heuss, and most importantly the gratitude of the British for his work for them during the war and in the Nazi trials.

And it was not an easy job to fill, with its international political implications. The German proposal to appoint a nonpolitical civil servant was vetoed by the Allied High Commissioners. The United States suggested an excellent man in Fabian von Schlabrendorff, but he refused on grounds of ill health. The French nominated Colonel Friedrich Wilhelm Heinz, information chief in the embryo defense ministry, but John disposed of this rival by having Ian Eland, his mistress' agent friend, put the finger on Heinz as the source of his espionage reports. Finally, after 15 months, 12 rejected nominees, and 10 wrangling sessions of the High Commission, the British quietly sponsored Otto John, for bad luck the thirteenth man.

The German lawyers who had defended Von Manstein and the Nuremberg accused were shocked. They complained to Minister of the Interior Heinemann that John was unscrupulous and altogether a bad choice. Heinemann replied that the British trusted John, and anyway the job was unimportant: Germany was in no position to keep secrets from the occupation powers.

U.S. approval was another Gordian knot. On 22 November 1950 High Commissioner McCloy cabled the Department of State from Frankfurt that the Federal Republic had requested HICOG to approve John's candidacy with all possible urgency, and that only the results of the Department's name check were needed to clear the way. A week later, at 1800 Washington time, 29 November, a cable over Dean Acheson's signature informed Frankfurt that conflicting information regarding Otto John "necessitates thorough investigation by Army G–2 of other sources. Results follow soonest." But on 1 December, at 0909, McCloy wired back:

> On basis of excellent data available here and in absence of any derogatory information and in view of urgency of making a decision and after approval by British and French, we approved appointment of Otto John on 29 November, prior to receipt of your telegram of 29 November.

The newly installed BfV president was again the center of discussions by the Allied Directorate when, on 7 March 1951, they took up the appointment of Vera Schwart, formerly a secretary of Admiral Canaris, as John's secretary. The United States and the UK raised no objections. But the French did, on the grounds that Vera, arrested by the Soviets in 1946, had turned informer for them the following year. The glandular dislike of French intelligence for John had been reflected in the comment of a Sureté chief on his appointment: he had exclaimed, in chorus with a Turkish colleague, "C'est impossible!"

Just how impossible a choice John was became increasingly apparent. Aside from his instability and his emotional political outlook, he was a poor administrator and lacked balanced judgment. U.S. intelligence saw him muddling through without the energy, imagination, or administrative ability to put the BfV on its feet. He had no patience with the painstaking detail necessary to effective intelligence operations. He was intrigued by special missions and fanciful projects which usually wound up putting the Office and the government in embarrassing, not to say ridiculous, positions.

One of the score of projects John laid on was Operation Maerchenwald. The good fairy of this Fabulous Wood was a buxom widow named Frau Baumann from Ansbach in Bavaria, confessed guardian of a vast Nazi treasure trove from which she was supposed to make monthly withdrawals to support indigent Nazi leaders in Switzerland and South America. The cache was somewhere in the Bavarian Alps, sometimes at the bottom of a lake, a very deep lake, the Frau said. John, taking her at her word, dispatched six green-jacketed BfV men to escort her to the treasure. She took them up into the Tyrolean mountains, where, according to an official report, she found the right blazed tree and the secret path of white pebbles, but was unable to find the stone slab covering the lever that opened the way to the cache.

While John was waiting in his Cologne command post for his men to report the find, U.S. operatives came to see him and showed him documents proving that his good fairy was a swindler, blackmail artist, public nuisance, and congenital liar, once inmate of an insane asylum. Nevertheless John summoned Frau Baumann to Cologne to reveal more details. Somewhat drunk, he had a two-hour seance with her.

By mid-1952 Bonn was rocking with gossip about his antics. Report after report reaching Adenauer's desk indicated that in his hatred of the Nazis John was not alert to the Communist danger, that he maintained relations with Communist sympathizers, that he was given to fits of melancholy brooding, and that he was increasingly taking to drink. But the Chancellor had no intention of lowering the boom on him until Germany achieved her sovereignty.

The BfV's serious operations were apparently in the hands of its de facto director, former General Staff officer Albert Radke. He was a close associate of General Reinhard Gehlen, who had headed the wartime General Staff's section for evaluating Eastern intelligence and in postwar Germany bossed a high-powered unofficial offensive espionage group. Gehlen distrusted John because of his record of defection to the British.

John's four years in office were extremely unpleasant. He was resented by senior police officials and other German civil servants as an outsider, as a stooge of his British sponsors, and as one who had deserted Germany in her hour of need. Rumors were growing that his days in the BfV were numbered, that his office would be replaced by Gehlen's organization. He may have brooded most over this prospect of being supplanted by Gehlen, whom he regarded as one of the military group responsible for the failure of the 1944 coup and so for Han's death by torture.

In May and June of 1954 he enjoyed the pleasant interlude of a trip to the United States. He was brought to Washington and shown the courtesies normally accorded the head of a foreign intelligence service. CIA officials dined him, and on 7 June he was briefed on general intelligence matters.

DETAILS IN A DEFECTION

John returned to the Federal Republic in fine fettle. Dr. Wohlgemuth, however, who visited him in Cologne on 9 July, insisted he appeared run down and prescribed pills. John, rather than argue about it, took them without visible effect, though later he tried to use this incident in his defense. On 8 and again on 12 July he was visited by Michael Winch, a discredited British-Soviet double agent. The subject of their conversations is not known. Frau John, who happened to be in Cologne, objected to Winch, probably because he was cadging meals and money.

John's twelve-year-old relationship with Wohlgemuth had been a matter of concern for some time. is reported to have warned him twice about friend Wowo, first in March

1953 and again in July 1954. After the first warning John is said to have detailed a BfV man, Von Berge, to watch him for a while, and on the second occasion to have given an "embarrassed" and conflicting account of his contacts with him. Before John's visit to the United States, a Berlin shopkeeper, Frau Anneliese Schroeder, showed police notes of a conversation with one Helmut Salewski, a close friend of Wohlgemuth's. Salewski told her Wowo kept a tape recorder hidden in his room and persuaded John to talk about secret matters when he visited him for evenings of women and drinking.

On 15 July the Johns flew to West Berlin for the services commemorating the decennial of the 20 July revolt. Beginning with a reception given by Oberburgmeister Reuter on the evening of 18 July, families and friends of the participants in the plot against the Nazi regime met for the purpose of unveiling a monument to the victims in the courtyard of the former OKW in the Bendlerstrasse. John and his wife took advantage of this opportunity to dine twice with his old school friend of Wiesbaden days, Wolfgang Hoffer, now a captain in the American CIC. Hoffer said that the Americans regarded John as a British agent, and that he himself couldn't stand the CIC any longer and wanted John to help him locate a job in Germany. He wanted nothing more to do with intelligence services.

An intelligence officer who spent considerable time with John during this convocation said he "lamented several times about the bad things people were saying about him and about attacks against him coming from Minister Robert Lehr and Herr Sauer. Shortly before he left Bonn to attend the Berlin festivities, he was called into [State Secretary] Ritter von Lex's office and was told they had just received a complaint from the Federal Chancellery accusing him of secretly joining the SPD. John said he was sick and tired of these rumors, and if a good opportunity presents itself he would seriously consider rejoining the Deutsche Lufthansa when it starts functioning again."[8]

In this mood he came upon a newspaper account of how Minister of the Interior Schroeder, his superior, planned drastic changes in the BfV as soon as West Germany obtained its sovereignty. He was reported to appear visibly shaken. At the commemorative exercises he made an exhibition of himself, sobbing loudly and denouncing two other mourners as Gestapo agents. Although the memories evoked of Hans' death ten years earlier were undoubtedly depressing, he had always been jovial and friendly at the memorial services of previous years.

Immediately after the ceremonies John declined to dine with his old friend Prince Louis Ferdinand, saying that he was meeting with some East Zone people. When Louis Ferdinand then suggested that Otto drop by his hotel afterwards for a nightcap, he gave a curt "No." This was about 1600 on 20 July.

John kept an engagement, however, with an elderly German couple, in-laws of an American acquaintance, at his hotel. In this interval between the memorial exercises in the Bendlerstrasse and his appointment with Wohlgemuth, he also saw Bonde-Henriksen, correspondent for the Danish paper *Berlingske Tidende,* the man who after eighteen months was to help him return from East Germany, and apparently expected to have a drink with him later in the evening.

A perhaps equivocal indication of his intention to come back that night was the fact that when he changed clothes he left papers and notes from his pockets in his hotel room. But he also had reservations for a return flight from Berlin, and his desk calendar in Cologne showed a future schedule of normal activities. Driving from his hotel, he stopped

[8] Lufthansa would not have taken him.

in at the Maison de France, a restaurant near Wohlgemuth's downtown office, in order, according to Erich Ollenhauer, to pick up there an answer to a proposal he had made Mendes-France that the Federal Republic's remilitarization plans be exposed to debate at the forthcoming Geneva Conference. The answer was not there.

For John's meeting and movements with Wohlgemuth the evidence consisted until recently mainly of his own account given after redefection, which begins by omitting these known preliminary activities, emphasizes a suspicious cup of coffee served him at the Wohlgemuth apartment, and ends in a theatrical invented scene wherein he awakens from a drugged sleep in an abandoned house and is threatened by Communists speaking with a Russian accent. But there were three important facts from other sources. Item one, Wohlgemuth telephoned the Charité Hospital in East Berlin that evening and said, "I shall come now with my good friend." Item two, he apparently intended, like John, to come back: he left in West Berlin his 10 suits of clothes, four apartments, five mistresses, and third wife. Later we shall look at other evidence of Wohlgemuth's intent made public in 1958 by the release of testimony given at John's treason trial. Item three, the customs officer on duty at the Sandkrug Bridge that night, Ernst Richard Hanke, who halted Wohlgemuth's sedan at the border, peered inside and saw that both occupants were awake and alert. When Hanke pointed out that the vehicle was about to enter the Soviet sector, a man of John's description replied, "Aber dort wollen wir doch hin—Well, that's where we want to go."

The Bonn Government insisted that John must have been abducted. They offered a reward of DM500,000 for conclusive information. A special Bundestag committee was established to investigate the affair. A variant on the abduction explanation was given by a U.S. intelligence cable:

> John was a damned fool caught in a well-baited trap. . . . He very likely overestimated his own position to the extent of believing that the Soviets would not dare harm him. He took and miscalculated a risk in pursuit of bait set by persons who evaluated correctly his psychology and his desire to score a major personal coup following heavy attacks on his office in recent Bundestag debates.

The suicide on 23 July of Otto's friend Hoffer, who had believed that the German secret police supposedly guarding John had actually been holding him under arrest, made the mystery a double one. John claimed, in a statement broadcast from East Berlin, that his friend had been driven to desperation by the CIC's insistence that he spy on him. Part of the German press said that Hoffer killed himself rather than face an inevitable investigation. The U.S. Army officially denied that he had been detailed to check up on John or on Wohlgemuth. U.S. intelligence had him feeling that the defection of his life-long friend shattered his whole intelligence career.

The British, publicly at any rate, stood by John. They denied on 5 August that any British official had been the source of an Associated Press story to the effect that they had dropped John ten months earlier; they considered such a report to be "skillful sabotage." John continued to have a surprisingly good British press,

At the other extreme were those who believed, on the grounds of John's vulnerability and associations, that he might have long since become a Soviet agent; and these included At least there were reports pointing to possible Communist pressures and preparation. Baron Wolfgang von und zu Putlitz, who first boasted and then denied having engineered the defection of Burgess and MacLean and who urged John on 16 March 1953 that he at

least confer with a Soviet officer about saving Germany from being caught in an East-West conflict, visited Bonn in the spring of 1954 and again in July, and on at least one of these occasions he met with John. Informed circles in East Berlin were reported in August to consider John's defection and that of the Bundestag deputy Karl Franz Schmidt-Wittmack to have been masterminded by Soviet General Ivan A. Serov and run from KGB headquarters in Karlshorst.[9] And a refugee who had worked for the East German Security Service claimed later to have heard Colonel Beater of the Service remark that two of his agents, Axel and Peter (the Rittwagens) were preparing in West Berlin for the defection or, if necessary, the abduction of Otto John, and that Beater had met at least once with Wohlgemuth and with Wolfgang Hoffer of the CIC.

Except to doggedly suspicious minds the baited-trap, drug-abduction, long-time-agent, and fleeing-wrongdoer theories were disproved and the main mysteries of the case cleared up by John's public appearance and a private conversation on 11 August. At a conference attended by 400 Western and Communist reporters in the East Berlin press building on Friedrichstrasse, he said that the West German government had become a mere instrument of American European policy, which was using Chancellor Adenauer to renazify and remilitarize Germany as a spearhead against the USSR, that there were secret clauses in the EDC treaty in this connection, that Adenauer and the militarists regarded the EDC as an interim device for restoring German military hegemony in Europe, that the Gehlen organization had stepped up its activities in France to this end, and that the Americans, in their hysterical fear of Communism, were preparing a new Hitler Crusade against the East that would leave Germany a mass of atomic ashes.

These standard theses of the Communist propaganda line were probably consonant with John's own anti-Nazi and anti-military obsession, reinforced in recent months by his growing feeling of being not appreciated in West Germany and not wanted in the government, even deliberately persecuted under the influence of the neo-Nazis. And if he felt guilt over his earlier desertion to the British, he could now choose the anti-Nazi East and still remain on German soil rather than "flee for a second time," as he later told the Danish correspondent Henrik Bonde-Henriksen.

After the press conference John had a 45-minute talk over glasses of beer with Gaston Coblentz of the New York *Herald Tribune* and two London paper correspondents, Karl Robson of the *News Chronicle* and his one-time boss and benefactor Sefton Delmer of the *Daily Express.* They were joined at the table in a private dining room of the press building by four Communist members of the Council for German Unity, but these made no attempt to control the conversation. They did not need to, the three Western correspondents agreed: John was saying of his own volition what they would have sought to have him say. The three gave him many opportunities to indicate by some sign that he was being held against his will, but although the talk around the table was going in several directions and it would have been easy, he did not do so.

John reiterated that he had crossed over voluntarily because of his long-smoldering unhappiness about renazification in West Germany. In reply to a question about Dr. Wohlgemuth's role, he said it was relatively unimportant—"he only established my contact with the Communist regime." John substantiated the theory that he had not intended to

[9] Peter Deriabin says that at the time of his own defection in September 1953 Soviet State Security was building up a file on John's dealings with the Nazis, and he suggests John was blackmailed into defecting by the Soviet threat to expose his pro-Nazi activities! (*The Secret World*, p. 197.)

remain in the Soviet Zone when he drove across the Sandkrug Bridge with Wowo. Asked whether he had decided in advance to stay, he replied: "No. My decision was made only after my talks with the Communist authorities. I came over to confirm that I would be able to stay on my terms. I was able to do so. I would have been free to return if I had wanted to."

John's motives do at this point seem understandable, and the main course of events clear. But as late as November 1958, perhaps because the picture was again confused by redefection, a senior U.S. intelligence officer in Germany was of the opinion that, "barring an unforeseeable stroke of good fortune, we doubt that we shall ever know the true circumstances which prompted Otto John's appearance in East Berlin."

THE WAY BACK

Shortly after his arrival in East Germany, John was reported to have made contact with Dr. Erich Correns, head of the National Front, and to have prepared for the Ministry of Interior a list of some 50 West German government officials possibly susceptible to defection inducements. On 14 August the West Berlin *Telegraf* reported his suggesting that former Field Marshal Friedrich von Paulus, who surrendered the German Sixth Army at Stalingrad, head a committee to "unveil the aggressive machinations of the National Socialist circles in West Germany."

A few weeks later, the East German government announced plans for a Ministry for German Unity to be headed by John. Its proposed purpose was to establish contact with persons in West German public life who were opposed to the Bonn government and thus encourage their opposition or provide them with an incentive to defect. The ministry never materialized, although John wrote to a number of prominent West German politicians urging them to take a stand against the U.S.-Adenauer policies.

On 19 September 1954 John was reported to be working on the All-German Committee of the East Zone government and also on the German Committee sponsored by the GDR Press and Information Office. It was learned later that he spent several weeks that fall in the USSR. Reports received in December 1954 indicated that he was planning to establish permanent residence in Leipzig, that he was working with the new East German Lufthansa, and that he was making preparations for a propaganda offensive to re-establish a constitutional monarchy in Germany and would soon make overtures to Prince Louis Ferdinand.

In March 1955 it was learned that he had been appointed permanent adviser to the National Council of the National Front and was touring the Soviet zone in official capacity, attending conferences of regional committees and issuing special directives for conducting anti-West propaganda. Late in October he was reported to be editor of a new publication, the *Berliner Politische Korrespondenz,* directed against the policies of the Bonn government and intended mainly for dissemination in West Berlin and the Federal Republic. He was also reported to be writing memoires.

But there had already been indications that John, disappointed with East Germany and with having been given only the position of "itinerant preacher for reunification," as he wrote his wife, was toying with the idea of returning to the West. This was the implication of a statement he made to Bonde-Henriksen in June 1955 that he was free to leave at any moment but hesitated because of fear of being arrested in West Germany. In a three-hour interview with the Danish correspondent, John said he would not have stayed on in East Germany if he thought the USSR desired war. Henriksen remarked, "It is a question of whether you would have been permitted to say 'Goodbye and thanks,' " and John replied, "I guess I would have known ways and means . . ." He concluded the

interview by saying: "I am a human being with the shortcomings and virtues of a human being. I can be accused of many things, but I have not failed the ideals of my youth. You may call me naive. Nevertheless, I am realistic and developments will prove me right."

In less than six months, however; perhaps particularly moved by a message from Prince Louis to the effect that if John really believed the things he was saying he could no longer be his friend, John arranged with Bonde-Henriksen to be picked up on Unter den Linden in front of the University at 1650 hours on 12 December 1955. At about 1635 he entered the University from Dorotheenstrasse, telling his two guards to wait at the gate since he had an appointment there. The guards let him go in alone. He walked through the buildings to where Henriksen was parked, waiting. Partially disguised in a muffler and dark glasses, he drove with Henriksen in the car bearing the Danish coat of arms through the Brandenburg Gate to the Victory Column and then to Tempelhof Airdrome. Bonde-Henriksen and Wiechmann from the regional BfV office flew with him to Wahn. From there he was driven to Bonn.

POST MORTEM

His fears of being arrested after his redefection were soon confirmed. He was charged on 18 January 1956 with treasonable conspiracy and high treason for his East Zone activities. His defense was that he thought it less damaging to West Germany, once he found himself in Communist hands through the drug-abduction routine, if he pretended to cooperate; if he refused, he would be brainwashed and forced to reveal state secrets of importance. He contended that he had had no chance to speak freely with Sefton Delmer and the other Western correspondents at his 11 August press conference or to convey any hint to anyone during the entire eighteen months that he was acting under compulsion.

The court was unimpressed. After a painstaking review of all the circumstances he was found guilty on two counts of treasonable conspiracy for his services to Eastern propaganda organizations. He was acquitted of betraying state secrets, but judged guilty of treasonable falsifications that would have been secret if true—his allegation of secret clauses in the EDC treaty and of activities of the Gehlen organization aimed at European hegemony. Sentenced to four years' imprisonment, he was released in July 1958 under an amnesty granted by President Heuss.

Wohlgemuth was brought to trial on treason charges but acquitted on 14 December 1958 by the West German Supreme Court. The court proceedings in the Wohlgemuth case have not yet been released, but the publication in 1958 of the official *Urteil* from the trial of Otto John[10] confirms the general outline of both men's motivations and actions drawn above and fills in some details.

The testimony of witnesses established that by the spring of 1954 John had become so apprehensive about attacks on him and his Office that he secured the promise of a legal position with an industrial firm against eventualities. It was clear to the court also that he had been genuinely, if unjustifiably, troubled by the idea that National Socialism might regain political power in Bonn. His political thinking, if somewhat vague, was certainly

[10] *Hochverrat und Staatsgefaerdung*, Band II (Karlsruhe: C. F. Mueller, 1958), pp. 77–150. The *Urteil* includes an exhaustive and impartial summary of the evidence and arguments of both prosecution and defense.

oriented toward the West and away from totalitarian forms of government. He distrusted military men, opposed remilitarization, and was shocked by the very thought of another war.

Witnesses pictured him as almost pathologically disturbed during his July visit to Berlin. He was convinced that the newspaper story of changes planned by the Interior Minister was aimed at him. At a lunch on 17 July, when someone remarked that only a war could resolve the current tension, he "shot up out of his chair." At the BfV Berlin office that afternoon he went to pieces, complaining with half-drunken vehemence about the lack of confidence in him. On 19 July at lunch he bemoaned the "growing influence of the Nazis" and went into a long reminiscence of the Third Reich and his own misunderstood role at Nuremberg. The memorial service on 20 July had an extraordinarily shattering effect on him.

With respect to any premeditation of his 20 July defection it was testified that he had booked a return flight to Cologne for 22 July, that he had refused his secretary's request for use of the official car on 21 July on the grounds that he would need it himself, that he told his chauffeur after dinner on 20 July that he was through with the car for the day but would call for it in the morning, and that as he left the hotel for the last time, although a clerk told him his wife was in the lobby, he did not say goodbye to her. His frequent letters to her from the East Zone referred again and again to his "sudden" decision and entreated her for understanding.

There was evidence also that the East German security service was unprepared for John's appearance in the East Zone and uncertain about his motives: a West German woman journalist whom it had imprisoned two years earlier on espionage charges and whom it supposed knew a good deal about John was brought before one of its officers in Halle just after 20 July and questioned as to whether she thought John's defection bona fide. Another West German journalist was told by John himself, in complete privacy on 13 May 1955, that the "number two Russian" in Karlshorst to whom he had offered his collaboration on 20 July was surprised, but made a kind of gentleman's agreement not to demand any secrets from him and to let him move about freely.

The testimony did not touch on the Hoffer mystery except to show that John had been inflating a jest of Hoffer's when he claimed the CIC had made him spy on him. From the bits of evidence available here it appears likely that Hoffer was disillusioned with intelligence intrigues, had made some indiscreet contacts in East Germany, and was afraid that his friend's defection would bring on an interrogation and exposure. John's attempt to blame his suicide on the CIC probably reflected a feeling of guilt for it on his own part.

Wohlgemuth, who did not make himself available as a witness, was pictured in the testimony as politically far to the left, announcing to all and sundry his conviction that Communism would come to power in western Europe within a few years. Nevertheless he had apparently not engaged in any legally actionable activities. With respect to his intentions in driving John across the Sandkrug Bridge, it was testified that when the two men left the office-apartment after the end of the Doctor's office hours that night, he was still wearing his white trousers and carrying only a trench coat, and that in the wee hours of 21 July he came back, alone, very much upset, and dashed to and fro through the house hastily packing a trunk.

He told the night nurse that John, whom he had introduced to some people in the East Zone, had unexpectedly decided to remain there, and that he himself might be suspected of wrongdoing and was therefore going back to stay at the Charité until things quieted down.

He left a note for the day nurse to the same effect, and told her to take care of the office and apartment. Between 4 and 5 a.m. he telephoned his attorney, gave him the same excited account, and asked him to take full powers over his property. Then he went to his mistress' house in Lietzenburger street, where he maintained a one-room apartment, and called her down to the street. Telling her what had happened, he suggested that his apartment might be searched and asked her to remove his camera, photographs, films, and books. At about five o'clock he stopped at the Uhland garage for gasoline, where the attendant noticed that he seemed to be in "even a bigger hurry than usual."

None of these people informed the police or Frau John, however, who first got from intelligence sources the news of John's probable defection, confirmed on 23 July by his own announcement over the East German radio:

> . . . I have taken a resolute step and made contact with the East Germans. I have been deprived of any basis for political activity in the Federal Republic. After I had been continually heckled in my office by the Nazis again rampant everywhere in political and even in public life, the Federal Minister of the Interior has now made any further work in my official position impossible for me by declaring to the press that with the coming of sovereignty he would have a free hand and be able "to entrust the protection of the constitution to persons who are truly above suspicion." . . . German policy has run into a blind alley . . . yet there is still a possibility of reunification. . . . I shall soon present my ideas and plans for German reunification to the German public.

Some students of the case are still convinced, in spite of the apparent adequacy of John's personal motivation, that he must nevertheless have defected under Soviet or more likely British control. To them the case can but remain a mystery; for although acquaintances like Winch, Putlitz, and Wohlgemuth may well have encouraged John's own obsessions, no evidence has come to light on how a supposed definitive control was exercised, and it is difficult to arrive even at a persuasive theoretical reconstruction of British or Soviet purposes consistent with the facts.

It seemed evident to the court, as it does to a reader of the intelligence files, that John's decision to approach the Communist authorities in the East Zone, made in a state of heightened neurotic tension and perhaps alcoholic befuddlement, derived from his frustration in what he considered his mission to stem the renazification of Germany and was precipitated by the imminent likelihood of his losing what position and influence he still had in the Federal Republic. When his initial Soviet contacts in Karlshorst led him, it seems probable, to believe he would be free of duress in the East and might be able to accomplish there what he could not in the West, he forthwith made his marriage of convenience with the Communists, in which any real position and influence yet escaped him and from which he eventually opted to return to his Western wife and friends.

GLOSSARY

ACCM	Alternative or Compensatory Control Measure
AFIO	Association of Former Intelligence Officers
AG	Attorney General
Aman	Agaf ha-Modi'in (Israeli military intelligence)
ANC	African National Congress
BDA	Battle Damage Assessment
BfV	Bundesamt für Verfassungsschutz (German equivalent of the FBI)
BMD	Ballistic Missile Defense
BND	Bundesnachrichtendienst (German foreign intelligence service)
BSO	Black September Organization
BW	Biological Weapons
CA	Covert Action
CAS	Covert Action Staff (CIA)
CBW	Chemical/Biological Warfare
CCP	Consolidated Cryptographic Program
CDA	Congressionally Directed Action
CE	Counterespionage
CHAOS	Code name for CIA illegal domestic spying
CI	Counterintelligence
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CIG	Central Intelligence Group
CMS	Community Management Staff
CNC	Crime and Narcotics Center (CIA)

COINTELPRO	FBI Counterintelligence Program
COMINT	Communications Intelligence
Corona	Codename for first U.S. spy satellite system
COS	Chief of Station (CIA)
COSPO	Community Open Source Program Office
CPA	Covert Political Action
CPSU	Communist Party of the Soviet Union
CSI	Committee on Intelligence Services (Britain)
CT	Counterterrorism
CTC	Counterterrorism Center (CIA)
CW	Chemical Weapons
D & D	Denial and Deception
DARP	Defense Airborne Reconnaissance Program
DAS	Deputy Assistant Secretary
DBA	Dominant Battlefield Awareness
DC	Deputies Committee (NSC)
DCD	Domestic Contact Division (CIA)
DCI	Director of Central Intelligence
D/CIA	Director of Central Intelligence Agency
DDA	Deputy Director of Administration (CIA)
DDCI	Deputy Director for Central Intelligence (DDCI)
DD/CIA	Deputy Director, Central Intelligence Agency
DDO	Deputy Director for Operations (CIA)
DDP	Deputy Director for Plans (CIA)
DDS&T	Deputy Director for Science and Technology (CIA)
DEA	Drug Enforcement Administration
DGSE	Directorie Génerale de la Sécurité Extérieure (French intelligence service)
DHS	Department of Homeland Security
DI	Directorate of Intelligence (CIA)
DIA	Defense Intelligence Agency
DIA/Humint	Defense Humint Service
DINSUM	*Defense Intelligence Summary*
DNI	Director of National Intelligence
DO	Directorate of Operations
DoD	Department of Defense
DOD	Domestic Operations Division (CIA)
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Treasury
DOS	Department of State
DP	Directorate of Plans (CIA)
DST	Directoire de Surveillance Territore (France)
ECHR	European Convention of Human Rights

ELINT	Electronic Intelligence
ENIGMA	Code machine used by the Germans during World War II
EO	Executive Order
EOP	Executive Office of the President
ETF	Environmental Task Force (CIA)
FARC	Fuerzas Armadas Revolucionarias in Colombia
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FISA	Foreign Intelligence Surveillance Act (1978)
FNLA	National Front for the Liberation of Angola
FOIA	Freedom of Information Act
FRD	Foreign Resources Division (CIA)
FSB	Federal'naya Sluzba Besnopasnoti (Federal Security Service, Russia)
GAO	General Accountability Office (Congress)
GCHQ	Government Communications Headquarters (the British NSA)
GEO	Geosynchronous Orbit
GEOINT	Geospatial Intelligence
GRU	Soviet Military Intelligence
GSG	German Counterterrorism Service
HEO	High Elliptical Orbit
HPSCI	House Permanent Select Committee on Intelligence
HUAC	House Un-American Activities Committee
HUMINT	Human Intelligence (assets)
I & W	Indicators and Warning
IAEA	International Atomic Energy Agency
IAF	Israel Air Force
IC	Intelligence Community
ICS	Intelligence Community Staff
IDF	Israeli Defense Force
IG	Inspector General
IMINT	Imagery Intelligence (photographs)
INR	Bureau of Intelligence and Research (Department of State)
INTELINK	An intelligence community computer information system
INTs	Collection disciplines (IMINT, SIGINT, OSINT, HUMINT, MASINT)
IOB	Intelligence Oversight Board (White House)
ISA	Israeli Security Agency
ISC	Intelligence and Security Committee (U.K.)
ISI	Inter-Services Intelligence (Pakistani intelligence agency)
IT	Information Technology
JCAE	Joint Committee on Atomic Energy
JCS	Joint Chiefs of Staff
JIC	Joint Intelligence Committee (U.K.)

JSOC	Joint Special Operations Command
JSTARS	Joint Surveillance Target Attack Radar Systems
KGB	Soviet Secret Police
KH	Keyhole (satellite)
LTTE	Tamil Tigers of Tamil Elam
MAGIC	Allied code-breaking operations against the Japanese in the World War II
MASINT	Measurement and Signatures Intelligence
MI5	Security Service (U.K.)
MI6	Secret Intelligence Service (U.K.)
MON	Memoranda of Notification
MONGOOSE	Code name for CIA covert actions against Fidel Castro of Cuba (1961–62)
Mossad	Israeli Intelligence Service
MPLA	Popular Movement for the Liberation of Angola
NAACP	National Association for the Advancement of Colored People
NBC	Nuclear, Biological, and Chemical (Weapons)
NCS	National Clandestine Service
NCIC	National Counterintelligence Center
NCTC	National Counterterrorism Center
NED	National Endowment for Democracy
NFIB	National Foreign Intelligence Board
NFIC	National Foreign Intelligence Council
NFIP	National Foreign Intelligence Program
NGA	National Geospatial-Intelligence Agency
NGO	Nongovernmental organization
NIA	National Intelligence Authority
NIC	National Intelligence Council
NID	*National Intelligence Daily*
NIE	National Intelligence Estimate
NIO	National Intelligence Officer
NOC	Nonofficial Cover
NPIC	National Photographic Interpretation Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council (White House)
NSCID	National Security Council Intelligence Directive
NTM	National Technical Means
OB	Order of Battle
OC	Official Cover
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
ONI	Office of Naval Intelligence

OPC	Office of Policy Coordination
OSD	Office of the Secretary of Defense
OSINT	Open-Source Intelligence
OSS	Office of Strategic Services
P & E	Processing and Exploitation
PDB	*President's Daily Brief*
PFIAB	President's Foreign Intelligence Advisory Board (White House)
PFLP	Popular Front for the Liberation of Palestine
PIJ	Palestinian Islamic Jihad
PLO	Palestine Liberation Organization
PM	Paramilitary
PRO	Public Record Office (U.K.)
RADINT	Radar Intelligence
RFE	Radio Free Europe
RL	Radio Liberty
SA	Special Activities Division (DO/CIA)
SAS	Special Air Service (U.K.)
SBS	Special Boat Service (U.K.)
SDO	Support to Diplomatic Operations
SHAMROCK	Code name for illegal NSA interception of cables
SIG	Senior Interagency Group
SIGINT	Signals Intelligence
SIS	Secret Intelligence Service (U.K., also known as MI6)
SISDE	Italian Intelligence Service
SMO	Support to Military Operations
SMS	Secretary's *Morning Summary* (Department of State)
SNIE	Special National Intelligence Estimate
SO	Special Operations (CIA)
SOCOM	Special Operations Command (Department of Defense)
SOE	Special Operations Executive (U.K.)
SOG	Special Operations Group (DO/CIA)
SOVA	Office of Soviet Analysis (CIA)
SSCI	Senate Select Committee on Intelligence
SVR	Russian Foreign Intelligence Service
TECHINT	Technical Intelligence
TELINT	Telemetery Intelligence
TIARA	Tactical Intelligence and Related Activities
TPED	Tasking, Processing, Exploitation, and Dissemination
UAV	Unmanned Aerial Vehicle (drone)
ULTRA	Code name for the Allied operation that deciphered the German ENIGMA code in World War II
UN	United Nations
UNITA	National Union for the Total Independence of Angola

UNSCOM	United Nations Special Commission
USIB	United States Intelligence Board
USTR	United States Trade Representative
VCI	Viet Cong Infrastructure
VENONA	Code name for SIGINT intercepts against Soviet spying in America
VOA	Voice of America
VX	A deadly nerve agent used in chemical weapons
WMD	Weapons of mass destruction

INDEX

ABOUT THE EDITOR AND CONTRIBUTORS

EDITOR

Loch K. Johnson is Regents Professor of Public and International Affairs at the University of Georgia and author of several books and over 100 articles on U.S. intelligence and national security. His books include *The Making of International Agreements* (1984); *A Season of Inquiry* (1985); *Through the Straits of Armageddon* (1987, coedited with Paul Diehl); *Decisions of the Highest Order* (1988, coedited with Karl F. Inderfurth); *America's Secret Power* (1989); *Runoff Elections in the United States* (1993, coauthored with Charles S. Bullock III); *America as a World Power* (1995); *Secret Agencies* (1996); *Bombs, Bugs, Drugs, and Thugs* (2000); *Fateful Decisions* (2004, coedited with Karl F. Inderfurth); *Strategic Intelligence* (2004, coedited with James J. Wirtz); *Who's Watching the Spies?* (2005, coauthored with Hans Born and Ian Leigh); *American Foreign Policy* (2005, coauthored with Daniel Papp and John Endicott); and *Seven Sins of American Foreign* Policy (2007). He has served as special assistant to the chair of the Senate Select Committee on Intelligence (1975–76), staff director of the House Subcommittee on Intelligence Oversight (1977–79), and special assistant to the chair of the Aspin-Brown Commission on Intelligence (1995–96). In 1969–70, he was an American Political Science Association Congressional Fellow. He has served as secretary of the American Political Science Association and President of the International Studies Association, South. Born in New Zealand and educated at the University of California, Johnson has taught at the University of Georgia since 1979, winning its Meigs Professorship for meritorious teaching and its Owens Award for outstanding accomplishments in the field of social science research. In 2000, he led the founding of the School of Public and

International Affairs at the University of Georgia. He is the senior editor of the international journal *Intelligence and National Security*.

CONTRIBUTORS

Matthew M. Aid is Managing Director in the Washington, DC, office of Citigate Global Intelligence and Security and coeditor of *Secrets of Signals Intelligence During the Cold War and Beyond* (2001).

James E. Baker sits on the U.S. Court of Appeals for the Armed Forces. He previously served as Special Assistant to the President and Legal Adviser to the National Security Council and as Deputy Legal Adviser to the NSC. He has also served as Counsel to the President's Foreign Intelligence Advisory Board, an attorney at the Department of State, a legislative aide to Senator Daniel Patrick Moynihan, and as a Marine Corps infantry officer. He is the coauthor with Michael Reisman of *Regulating Covert Action* (Yale University Press, 1992).

David M. Barrett is Associate Professor of Political Science at Villanova University and author of *Congress and the CIA* (Kansas, 2005).

Hans Born is a senior fellow in democratic governance of the security sector at the Geneva Centre for Democratic Control of the Armed Forces (DCAF). He is an external member of the crisis management and security policy faculty of the Federal Institute of Technology and a guest lecturer on governing nuclear weapons at the UN Disarmament Fellowship Programme. He has written, co-authored, and co-edited various books on international relations and security policy, including the Inter-Parliamentary Union Handbook on *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices* (Geneva: IPU/DCAF, 2003, translated in 30 languages); *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005, translated in 10 languages); *Who is Watching the Spies? Establishing Intelligence Agency Accountability* (Dulles, VA: Potomac Publishers, 2005); *Civil-Military Relations in Europe: Learning from Crisis and Institutional Change* (London: Routledge, 2006); and *The Double Democratic Deficit: Parliamentary Accountability and the Use of Force under International Auspices* (London: Ashgate Publishers: Aldershot).

A. Denis Clift is President of the Department of Defense Joint Military Intelligence College. He was born in New York City and educated at Friends Seminary, Phillips Exeter Academy (1954), Stanford University (B.A., 1958), and the London School of Economics and Political Science (M.Sc., 1967). He began a career of public service as a naval officer in the Eisenhower and Kennedy administrations and has served in military and civilian capacities in ten administrations, including thirteen successive years in the Executive Office of the President and the White House. From 1971–76, he served on the National Security

Council staff. From 1974–76, he was head of President Ford's National Security Council staff for the Soviet Union and Eastern and Western Europe. From 1977–81, he was Assistant for National Security Affairs to the Vice President. From 1991–94, he was Chief of Staff, Defense Intelligence Agency. From 1963–66, he was the editor of the U.S. Naval Institute *Proceedings*. His published fiction and nonfiction include the novel *A Death in Geneva* (Ballantine Books, Random House), *Our World in Antarctica* (Rand McNally), *With Presidents to the Summit* (George Mason University Press), and *Clift Notes: Intelligence and the Nation's Security* (JMIC Writing Center Press).

William J. Daugherty holds a doctorate in government from the Claremont Graduate School and is Associate Professor of government at Armstrong Atlantic State University in Savannah, Georgia. A retired senior officer in the CIA, he is also the author of *In the Shadow of the Ayatollah: A CIA Hostage in Iran* (Annapolis, 2001) and *Executive Secrets: Covert Action and the Presidency* (Kentucky, 2004).

Jack Davis served in the CIA from 1956 to 1990 as analyst, manager, and teacher of analysts. He now is an independent contractor with the Agency, specializing in analytic methodology. He is a frequent contributor to the journal *Studies in Intelligence*.

Stuart Farson is Lecturer, Political Science Department, Simon Fraser University, Vancouver/Surrey, Canada. He is a former Secretary-Treasurer of the Canadian Association for Security and Intelligence Studies, and served as Director of Research for the Special Committee of the House Commons (Canada) on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act. He has numerous articles on security, intelligence, and policing issues and is the coeditor of *Security and Intelligence in a Changing World* (with David Stafford and Wesley K. Wark, Cass, 1991).

Timothy Gibbs is a final-year doctoral student in history at Robinson College, Cambridge University, and a member of the Cambridge University Intelligence Seminar. He is also a former Visiting Scholar at the University of Georgia. His doctoral dissertation, titled *British and American Intelligence and the Atom Spies*, was submitted in the summer of 2006 and was supervised by Professor Christopher Andrew.

Peter Gill is Reader in Politics and Security, Liverpool John Moores University, Liverpool, United Kingdom. He is coauthor of *Introduction to Politics* (1988, 2nd ed.) and *Intelligence in an Insecure World* (2006). He is currently researching the control and oversight of domestic security in intelligence agencies.

Harold M. Greenberg graduated with a B.A. in history from Yale University in 2005. At Yale, he participated in the Studies in Grand Strategy program, and he has recently published research on CIA covert action in the 1950s. He now works as a legislative aide in the U.S. House of Representatives.

Daniel S. Gressang IV is Professor at the Joint Military Intelligence College (JMIC) in Washington, DC, and serves concurrently as the National Security Agency/National Cryptologic School of Liaison to JMIC. He has researched, written, and lectured extensively on terrorism and counterinsurgency. His research focuses primarily on the application of complex adaptive systems perspectives to understanding the dynamics of terror and other forms of unconventional warfare. In 2004, he was designated Intelligence Community Officer by the Director of Central Intelligence.

Glenn Hastedt received his doctorate in political science from Indiana University. Until recently he was Professor and Chair of the Political Science Department at James Madison University. He is now chair of the Justice Studies Department there. Among his publications is *American Foreign Policy: Past, Present, Future*, 6th ed. (Prentice Hall).

John Hollister Hedley, during more than thirty years at CIA, edited the *President's Daily Brief*, briefed the *PDB* at the White House, served as Managing Editor of the *National Intelligence Daily*, and was Chairman of the CIA's Publications Review Board. Now retired, Hedley has taught intelligence at Georgetown University and serves as a consultant to the National Intelligence Council and the Center for the Study of Intelligence.

Michael Herman served from 1952 to 1987 in Britain's Government Communications Headquarters, with secondments to the Cabinet Office and the Ministry of Defence. Since retirement he has written extensively on intelligence matters, with official clearance. He has had academic affiliations with Nuffield and St. Antony's Colleges in Oxford and is Founder Director of the Oxford Intelligence Group and Honorary Departmental Fellow at Aberystwyth University. In 2005 he received the degree of Honorary D.Litt from Nottingham University. He is a leading British intelligence scholar and author of *Intelligence Power in Peace and War* (Cambridge, 2001).

Frederick P. Hitz is Lecturer (Diplomat in Residence) in Public and International Affairs, Woodrow Wilson School, Princeton University.

Max M. Holland is the author of *The Kennedy Assassination Tapes* (Knopf, 2004).

Arthur S. Hulnick is Associate Professor of International Relations at Boston University. He is a veteran of thirty-five years of intelligence service, including seven years in Air Force Intelligence and twenty-eight years in the CIA. He is author of *Fixing the Spy Machine* (Praeger, 1999) and *Keeping Us Safe* (Praeger, 2004).

Rhodri Jeffreys-Jones is Professor of American History at the University of Edinburgh. The author of several books on intelligence history, he is currently completing a study of the FBI.

Ephraim Kahana is Professor of Political Science and faculty member in the Western Galilee College, Acre, Israel. He teaches courses on international relations, national security and intelligence, and foreign policy in the National Security Program in the University of Haifa. Kahana has written numerous papers on intelligence and foreign policy. His most recent book is the *Historical Dictionary of Israeli Intelligence* (2006).

Patrick Radden Keefe is a graduate of the School of Law at Yale University and is presently a Fellow with the Century Foundation in New York City. He is the author of *Chatter: Uncovering the Echelon Surveillance Network and the Secret World of Global Eavesdropping* (Random House, 2006), and has published essays in *The New York Review of Books*, *The New York Times Magazine*, the *New York Times*, the *Boston Globe*, the *Yale Journal of International Law*, *Legal Affairs*, *Slate*, and *Wired*. He has been a Marshall Scholar and a 2003 fellow at the Dorothy and Lewis B. Cullman Center for Scholars and Writers at the New York Public Library.

Jennifer D. Kibbe is Assistant Professor of Government at Franklin and Marshall College. Between 2002 and 2004, she was a postdoctoral fellow at the Brookings Institution. Her research interests include U.S. foreign policy, intelligence and covert action, presidential decision making, and political psychology. She has published work on U.S. policy in Iraq and the Middle East, and the military's involvement in covert actions.

Katharina von Knop is a doctoral candidate in Political Science at Leopold-Franzens University in Innsbruck, Austria, specializing in counter- and antiterrorism, and coeditor with Heinrich Neisser and Martin van Creveld of *Countering Modern Terrorism: History, Current Issues, and Future Threats* (2005).

Lawrence J. Lamanna is a doctoral candidate in the School of Public and International Affairs at the University of Georgia. He holds an M.A. from Yale University and a B.A. from the University of Notre Dame.

Ian Leigh is Professor of Law and Codirector of the Human Rights Centre at the University of Durham. He lives in Durham, England.

Kristin M. Lord is Associate Dean at George Washington University's Elliott School of International Affairs. In 2005–2006, she was a Council on Foreign Relations International Affairs Fellow and Special Adviser to the Under Secretary of State for Democracy and Global Affairs. Lord is the author of *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security Democracy or Peace* (SUNY Press, 2006); coeditor, with Bernard I. Finel, of *Power and Conflict in the Age of Transparency* (Palgrave Macmillan, 2000); and the author of numerous book chapters, articles, and papers on international politics and security. Lord received her doctorate in government from Georgetown University.

Minh A. Luong is Assistant Director of International Security Studies at Yale University, where he teaches in the Department of History. He also serves as adjunct Assistant Professor of Public Policy at the Taubman Center at Brown University.

Cynthia M. Nolan earned a doctorate at American University in the School of International Service, researching intelligence oversight. She is a former officer in the Directorate of Operations in the CIA and has published in the *International Journal of Intelligence and Counterintelligence*.

Kevin A. O'Brien is a former research associate with the Canadian Institute of Strategic Studies and is currently a senior analyst for RAND Europe.

Mark Phythian is Professor of International Security and Director of the History and Governance Research Institute at the University of Wolverhampton, United Kingdom. He is the author of *Intelligence in an Insecure World* (2006, with Peter Gill), *The Politics of British Arms Sales Since 1964* (2000), and *Arming Iraq* (1997), as well as numerous journal articles on intelligence and security issues.

Harry Howe Ransom is Professor Emeritus of Political Science at Vanderbilt University. He has a B.A. from Vanderbilt and an M.A. and Ph.D. from Princeton University. He was a Congressional Fellow of the American Political Science Association and a Fellow of the Woodrow Wilson International Center for Scholars. He taught at Princeton, Vassar College, Michigan State University, Harvard University, and the University of Leeds. His books include *Central Intelligence and National Security* (1958), *Can American Democracy Survive Cold War?* (1963), and *The Intelligence Establishment* (1970).

Jeffrey T. Richelson is Senior Fellow with the National Security Archive in Washington, DC, and author of *The Wizards of Langley*, *The U.S. Intelligence Community*, *A Century of Spies*, and *America's Eyes in Space*, as well as numerous articles on intelligence activities. He received his doctorate in political science from the University of Rochester and has taught at the University of Texas, Austin, and the American University, Washington, DC. He lives in Los Angeles.

Jerel A. Rosati is Professor of Political Science and International Studies at the University of South Carolina since 1982. His area of specialization is the theory and practice of foreign policy, focusing on the U.S. policy-making process, decision-making theory, and the political psychological study of human cognition. He is the author and editor of five books and over forty articles and chapters. He has received numerous outstanding teaching awards. He has been Visiting Professor at Somalia National University in Mogadishu and Visiting Scholar at China's Foreign Affairs College in Beijing. He also has been a Research Associate in the Foreign Affairs and National Defense Division of the Library of Congress's Congressional Research Service, President of the International

Studies Association's Foreign Policy Analysis Section, and President of the Southern region of the International Studies Association.

Richard L. Russell is Professor of national security studies at the National Defense University. He is also an adjunct associate professor in the Security Studies Program and research associate in the Institute for the Study of Diplomacy at Georgetown University. He previously served as a CIA political-military analyst. Russell is the author of *Weapons Proliferation and War in the Greater Middle East: Strategic Contest* (2005).

Frederick A. O. Schwarz Jr. received an A.B. from Harvard University and J.D. from Harvard Law School, where he was an editor of the *Law Review*. After a year's clerkship with Hon. J. Edward Lumbard, U.S. Court of Appeals for the Second Circuit, he worked one year for the Nigerian government as Assistant Commissioner for Law Revision under a Ford Foundation grant. He joined the New York City law firm of Cravath, Swaine and Moore in 1963 and was elected a partner in 1969. From 1975 through mid-1976, he served as Chief Counsel to the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the Church Committee); from 1982–89, he served as Corporation Counsel and head of the Law Department of the City of New York. In 1989, he chaired the New York City Charter Revision Commission.

James M. Scott is Professor and Chair of the Department of Political Science at Oklahoma State University. His areas of specialization include foreign policy analysis and international relations, with particular emphasis on U.S. foreign policy making and the domestic sources of foreign policy. He is author or editor of four books, over forty articles, book chapters, review essays, and other publications. He has been President of the Foreign Policy Analysis section and President of the Midwest region of the International Studies Association, where he has also served as conference organizer for both sections and has been a two-time winner of the Klingberg Award for Outstanding Faculty Paper at the ISA Midwest Annual Meeting. Since 1996, he has received over two dozen awards from students and peers for his outstanding teaching and research, including his institution's highest awards for scholarship in 2000 and 2001. Since 2005, he has been Director of the Democracy and World Politics Summer Research Program, a National Science Foundation Research Experience for Undergraduates.

Len Scott is Professor of International Politics at the University of Wales, Aberystwyth, where he is Director of the Centre for Intelligence and International Security Studies. Among his recent publications are *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows* (2004, coedited with Peter Jackson) and *Planning Armageddon: Britain, the United States and the Command of Nuclear Forces, 1943–1964* (2000, coedited with Stephen Twigge).

Katherine A. S. Sibley is Professor and Chair of the History Department at St. Joseph's University. She is currently working on a biography of Florence Kling

Harding, titled *America's First Feminist First Lady*. Sibley's work will revise the typical portrait of Mrs. Harding as manipulative, unhappy wife, casting new light on her public and private life. In 2004, Sibley published *Red Spies in America: Stolen Secrets and the Dawn of the Cold War* with the University Press of Kansas. She is also the author of *The Cold War* (1998) and *Loans and Legitimacy: The Evolution of Soviet-American Relations, 1919–1933* (1996). Her work has appeared in journals including *American Communist History*, *Peace and Change*, and *Diplomatic History*, and she also serves as book review editor for *Intelligence and National Security*. She is a three-term Commonwealth Speaker for the Pennsylvania Humanities Council.

Jennifer Sims is Director of Intelligence Studies and Visiting Professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service. She also consults for the U.S. government and private sector on homeland security and intelligence related matters. Prior to this, Sims was Research Professor at Johns Hopkins University's Nitze School of Advanced International Studies in Washington, DC (Fall 2001–Summer 2003). She has served as defense and foreign policy adviser to Senator John Danforth (1990–94), a professional staff member of the Senate Select Committee on Intelligence (1991–94), Deputy Assistant Secretary of State for Intelligence Coordination (1994–98), and as the Department of State's first Coordinator for Intelligence Resources and Planning in the office of the Under Secretary for Management. In 1998 Sims was awarded the U.S. Intelligence Community's Distinguished Service Medal. She received her B.A. degree from Oberlin College and her M.A. and Ph.D. in national security studies from Johns Hopkins University in 1978 and 1985, respectively. She is the author of a number of books and articles on intelligence and arms control. The most recent of these include "Foreign Intelligence Liaison: Devils, Deals and Details," *International Journal of Intelligence and Counterintelligence Affairs* (Summer 2006); *Transforming US Intelligence,* coedited with Burton Gerber (Georgetown University Press, 2005); "Transforming U.S. Espionage: A Contrarian's Approach," *Georgetown Journal of International Affairs* (Winter/Spring 2005); "Domestic Factors in Arms Control: The U.S. Case," in Jeffrey A Larson (ed.), *Arms Control: Cooperative Security in a Changing Environment* (Lynne Rienner, 2002); "What Is Intelligence? Information for Decision-Makers," in Roy Godson, Ernest R. May, and Gary Schmitt, *U.S. Intelligence at the Crossroads* (Brassey's, 1995); "The Cambridge Approach Reconsidered," *Daedalus* 120 (Winter 1991); and *Icarus Restrained: An Intellectual History of American Arms Control* (Westview Press, 1990).

Robert David Steele is CEO of OSS.Net, an international open source intelligence provider. As the son of an oilman, a Marine Corps infantry officer, and a clandestine intelligence case officer for the CIA, he has spent over twenty years abroad in Asia and Central and South America. As a civilian intelligence officer he spent three back-to-back tours overseas, including one tour as one of the first officers assigned full-time to terrorism, and three headquarters tours in offensive

counterintelligence, advanced information technology, and satellite program management. He resigned from the CIA in 1988 to be the senior civilian founder of the Marine Corps Intelligence Command. He resigned from the Marines in 1993. He is the author of three works on intelligence, as well as the editor of a book on peacekeeping intelligence. He has earned graduate degrees in international relations and public administration, is a graduate of the Naval War College, and has a certificate in Intelligence Policy. He is also a graduate of the Marine Corps Command and Staff Course and of the CIA's Mid-Career Course 101.

John D. Stempel is Senior Professor of International Relations at the University of Kentucky's Patterson School of Diplomacy and International Commerce, where he was Associate Director (1988–93) and Director (1993–2003). He came to the University of Kentucky following a 24-year career in the U.S. Foreign Service. There he focused on political and economic affairs, with overseas assignments in Africa (Guinea, Burundi, Zambia), Iran, and India, concluding with three years as U.S. Consul General in Madras. His Middle East service (1975–79) in Tehran provided the material for his book *Inside the Iranian Revolution*. His subsequent academic writings have focused on religion and diplomacy, intelligence and diplomacy, and American views of negotiation. His Washington assignments featured duty for both the State and Defense Departments, including a two-year tour as Director of the State Department's Crisis Center. He has taught at George Washington and American Universities, plus two years as Diplomat in Residence at the U.S. Naval Academy, Annapolis. Stemple is a member of the New York Council on Foreign Relations and is listed in *Who's Who in the World* and *Who's Who in America*. He holds an A.B. degree from Princeton University and M.A. and Ph.D. degrees from the University of California at Berkeley.

Stan A. Taylor is an Emeritus Professor of Political Science at Brigham Young University in Provo, Utah. He has taught in England, Wales, and New Zealand and in 2006 was a visiting professor at the University of Otago in Dunedin, New Zealand. He is founder of the David M. Kennedy Center for International Studies at Brigham Young University. He writes frequently on intelligence, national security, and U.S. foreign policy.

Athan Theoharis is Professor of History at Marquette University whose research has focused on government secrecy, Cold War politics, and the history of the FBI. He is the author, coauthor, and editor of eighteen books, including *The FBI and American Democracy* (2004), *Chasing Spies* (2002), *A Culture of Secrecy* (1998), and *The FBI: A Comprehensive Reference Guide* (1998). He has received numerous awards, including the American Bar Association's Gavel Award and selection as a fellow by the Wisconsin Academy of Arts, Sciences, and Letters.

Gregory F. Treverton is senior analyst at the RAND Corporation. Earlier, he directed RAND's Intelligence Policy Center and its International Security and Defense Policy Center, and he is Associate Dean of the Pardee RAND Graduate School. His recent work has examined at terrorism, intelligence, and law

enforcement, with a special interest in new forms of public-private partnership. He has served in government for the first Senate Select Committee on Intelligence, handling Europe for the National Security Council, and most recently as vice chair of the National Intelligence Council, overseeing the writing of America's National Intelligence Estimates. He holds an A.B. *summa cum laude* from Princeton University, a master's in public policy, and Ph.D. in economics and politics from Harvard University. His latest books are *Reshaping National Intelligence for an Age of Information* (Cambridge University Press, 2001), and *New Challenges, New Tools for Defense Decisionmaking* (edited, RAND, 2003).

Michael A. Turner is a political scientist who has taught international relations and national security matters in San Diego, California, for the past twelve years. Before that, he spent over fifteen years in various positions within the CIA. Turner is the author of *Why Secret Intelligence Fails* (2005; 2006) and the *Historical Dictionary of United States Intelligence* (2006).

Michael Warner serves as Historian for the Office of the Director of National Intelligence.

Nigel West is a military historian specializing in security and intelligence topics. He is the European editor of the *World Intelligence Review* and is on the faculty at the Center for Counterintelligence and Security Studies in Washington, DC. He is the author of more than two dozen works of nonfiction and recently edited *Guy Liddell Diaries*.

Reg Whitaker is Distinguished Research Professor Emeritus, York University, and Adjunct Professor of Political Science, University of Victoria, Canada. He has written extensively on Canadian and international security and intelligence issues.

James J. Wirtz is Professor in the Department of National Security Affairs at the Naval Postgraduate School, Monterey, California. He is Section Chair of the Intelligence Studies Section of the International Studies Association and President of the International Security and Arms Control Section of the American Political Science Association. Wirtz is the series editor for *Initiatives in Strategic Studies: Issues and Policies*, published by Palgrave Macmillan.

Amy B. Zegart is Associate Professor of Public Policy at the University of California, Los Angeles. A specialist on national and homeland security, she has served on the National Security Council staff, as a foreign policy advisor to the Bush-Cheney 2000 presidential campaign, and as a consultant to California state and local homeland security agencies. She has published articles in leading academic journals, including *International Security* and *Political Science Quarterly*, and is the author of *Flawed by Design: The Origins of the CIA, JCS, and NSC* (Stanford, 1999). She received her Ph.D. in political science from Stanford, where she studied under Condoleezza Rice, and an A.B. in East Asian Studies from Harvard University.

STRATEGIC INTELLIGENCE

STRATEGIC INTELLIGENCE

2

THE INTELLIGENCE CYCLE: THE FLOW OF SECRET INFORMATION FROM OVERSEAS TO THE HIGHEST COUNCILS OF GOVERNMENT

Edited by
Loch K. Johnson

Intelligence and the Quest for Security

PRAEGER SECURITY INTERNATIONAL
Westport, Connecticut • London

Library of Congress Cataloging-in-Publication Data

Strategic intelligence / edited by Loch K. Johnson.
p. cm.—(Intelligence and the quest for security, ISSN 1932-3492)
Includes bibliographical references and index.
ISBN 0-275-98942-9 (set : alk. paper)—ISBN 0-275-98943-7 (vol. 1 : alk. paper)—
ISBN 0-275-98944-5 (vol. 2 : alk. paper)—ISBN 0-275-98945-3 (vol. 3 : alk. paper)—
ISBN 0-275-98946-1 (vol. 4 : alk. paper)—ISBN 0-275-98947-X (vol. 5 : alk. paper)
1. Military intelligence. 2. Intelligence service—Government policy. I. Johnson, Loch K., 1942–

UB250.S6385 2007
327.12—dc22 2006031165

British Library Cataloguing in Publication Data is available.

Library of Congress Catalog Card Number: 2006031165
ISBN: 0-275-98942-9 (set)
0-275-98943-7 (vol. 1)
0-275-98944-5 (vol. 2)
0-275-98945-3 (vol. 3)
0-275-98946-1 (vol. 4)
0-275-98947-X (vol. 5)
ISSN: 1932-3492

First published in 2007

Praeger Security International, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the Untied States of America

The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE

THIS FIVE-VOLUME SERIES IN INTELLIGENCE IS SOMETHING of a landmark in the study of intelligence. Thirty years ago, one would have been hard-pressed to find enough good articles on the subject to fill two volumes, let alone five. In those three decades since 1975, however, the study of intelligence has grown considerably. Today there are several solid professional journals in the field, including the premier publications *Intelligence and National Security* (published in the United Kingdom), *International Journal of Intelligence and Counterintelligence* (the United States), and *Studies in Intelligence* (from the Central Intelligence Agency, in both classified and unclassified form). In just the past two years, bulging anthologies on the general topic "strategic intelligence," as well as a "handbook" on intelligence and a collection of chapters within the more specialized niche of "intelligence and ethics" have appeared, along with a tidal wave of books and articles on one aspect or another of this subject (see the bibliographic essay in volume 1).

Except in times of scandal (Watergate in 1973, CIA domestic spying in 1974, the Iran-*contra* affair in 1987), one could find in this earlier era little newspaper coverage of intelligence activities, so tightly held were these operations by the government. Now, fueled by the events of the September 11, 2001, terrorist attacks and the erroneous prediction in 2002 that weapons of mass destruction (WMDs) were being developed and stockpiled by Iraq, hardly a week goes by without reports on intelligence in the *New York Times* and other leading newspapers. These days, the *Atlantic Monthly* and the *New Yorker*, America's top literary magazines, visit the subject with some regularity, too. The latter has hired Seymour M. Hersh, the nation's most well-known investigative reporter with an intelligence beat.

Intelligence studies has come of age.

Certainly the chapters in these volumes display a breadth of inquiry that suggests an admirable vibrancy in this relatively new field of study. Presented here are empirical inquiries, historical treatments, theoretical frameworks, memoirs, case studies, interviews, legal analyses, comparative essays, and ethical assessments. The authors come from the ranks of academe (twenty-five); the intelligence agencies (thirteen); think tanks (seven); Congress, the State Department, and the National Security Council (three); and the legal world (three).[1] Over a quarter of the contributors are from other nations, including Canada, England, Germany, Israel, Scotland, Switzerland, and Wales. The American writers come from every region of the United States. As a collective, the authors represent a wide range of scholarly disciplines, including computer science, history, international affairs, law, sociology, political science, public administration, public policy studies, and strategic studies. Many of the contributors are from the ranks of the top intelligence scholars in the world; a few young ones stand at the gateway to their academic careers.

Notable, too, is the number of women who have entered this field of study. Thirty years ago, it would have been rare to find one or two women writing on this subject. Seven have contributed chapters to these pages, and another two wrote documents that appear in the appendixes. This is still fewer than one would like, especially in light of the major contribution women have made as intelligence officers. One thinks of the heroic efforts of British women in code breaking and in the Special Operations Executive during World War II, and the American women who contributed so much to the analytic efforts of the Office of Strategic Studies (OSS) during that same war. At least, though, the number attracted to the scholar study of intelligence appears to be rapidly expanding.

The end result of this mix is a landscape illuminated by a variety of methods and appreciations—a rich research trove that examines all the key aspects of intelligence. In addition, each of the volumes contains backup materials in the appendixes. These documents provide the reader with access to significant primary and secondary sources referred to in the chapters.

The volumes are organized according to the major topics of studies in the field. The first volume, titled *Understanding the Hidden Side of Government*, introduces the reader to methods commonly used in the study of intelligence. It imparts, as well, a sense of the "state of the discipline," beginning with a bibliographic essay (by the editor) and continuing with an examination of specific approaches scholars have adopted in their inquiries into this especially difficult discipline, where doors are often shut against outsiders.

In the bibliographic essay that opens the volume, I argue that the literature on intelligence has mushroomed over the past thirty years. Some of this literature is unreliable, but much of it is of high quality. Amy B. Zegart follows my chapter with an important caveat: the literature may be more voluminous these days, but intelligence studies as an academic field has yet to be accepted as a vital part of national security scholarship. The mainstream journals of history, international

affairs, and political science have still regarded the study of intelligence as a marginal pursuit. In this regard, Zegart points out, there is a major disconnect between academic scholarship and those who make decisions in Washington, London, and other capitals around the world.

Following this introduction, Len Scott and Timothy Gibbs look at methods that have been used to study intelligence in the United Kingdom; Stuart Farson and Reg Whitaker in Canada; and Michael Warner in the United States. The volume then turns to a more specific inquiry into the central question of how intelligence is interpreted by professionals—the issue of analysis—explored by John Hollister Hedley. An overview of the sometimes turbulent relationship between intelligence officers and the policy makers they serve is explored by James J. Wirtz; and British scholar Peter Gill recalls the failures associated with the 9/11 attacks and the poor judgments about Iraqi WMDs, in hopes of extracting lessons from these intelligence disasters. In the next chapter, the youngest scholar represented in this collection, Harold M. Greenberg, takes us back in time with a remembrance of the legendary CIA officer and Yale history professor Sherman Kent, often known as the dean of CIA analysts. Kristin Lord rounds out the first volume with a look forward into future prospects for a more transparent world—the ultimate goal of intelligence.

As with each of the books, Volume 1 has a set of appendixes designed to supplement the original chapters with supportive materials from government documents and other sources. Appendix A contains the relevant intelligence excerpts from the National Security Act of 1947—the founding charter for the modern American intelligence establishment. Appendix B provides a history of U.S. intelligence since 1947, prepared for the Aspin-Brown Commission in 1995–96 by staff member Phyllis Provost McNeil. These two documents present a contextual backdrop for the Volume 1 chapters. Appendix C provides "wiring diagrams" of the intelligence community, that is, organizational blueprints for the sixteen agencies and related entities. One chart displays the community as it is today, and another displays how it looked in 1985. As the contrast between the two illustrates, the events of September 11, 2001, have led to a larger and more complex intelligence apparatus in the United States. Appendix D shows a photograph of the CIA Headquarters Building, as an example of what one of the secret agencies actually looks like from an aerial perspective. The white dome in the foreground is an assembly hall seating around 600 people and to its left is the main entrance to the original CIA headquarters, built during the Eisenhower years. Behind this older wing is the new green-glass structure erected during the Reagan administration, often known as the Casey addition because William J. Casey was the Director of Central Intelligence (DCI) at the time of its construction during the 1980s.

Appendix E lists the top leadership in the America's intelligence community: the DCIs from 1947–2005 and today's DNI. Included here as well are the leaders in Congress who have been responsible for intelligence accountability in the past, along with the current members of the two congressional Intelligence

Committees: the Senate Select Committee on Intelligence (SSCI, or "sissy" in the unflattering and sometimes true homophone of Capitol Hill vernacular) and the House Permanent Select Committee on Intelligence (HPSCI or "hipsee"). Appendix F presents a 1955 statement from historian and CIA analyst Sherman Kent about the need for a more robust intelligence literature. He would probably be amazed by how much is being written on this subject now. Appendix G offers an overview on the purpose and challenges of intelligence, drawn from the introductory chapters of the Aspin-Brown Commission Report. Finally, Appendix H provides an opening glimpse into the subject of counterintelligence, a world of counterspies and betrayal taken up more fully in Volume 4.

With the second volume, titled *The Intelligence Cycle: The Flow of Secret Information From Overseas to the Highest Councils of Government*, the focus shifts from a broad overview of intelligence to a more detailed examination of its core mission: the collection, analysis, and dissemination of information from around the world. The National Security Act of 1947, which created America's modern intelligence establishment, made it clear that the collection, analysis, and dissemination of information would be the primary duty of the intelligence agencies. As Allen Dulles—the most famous DCI (America's top intelligence official, until this title changed to director of National Intelligence or DNI in 2005)—put it, the intelligence agencies were expected "to weigh facts, and to draw conclusions from those facts, without having either the facts or the conclusions warped by the inevitable and even proper prejudices of the men whose duty it is to determine policy."[2] The collection and interpretation of information, through espionage and from the public record, would be the primary responsibility of America's secret agencies.

At the heart of this mission lies the so-called intelligence cycle. Professional intelligence officers define the cycle as "the process by which information is acquired, converted into intelligence, and made available to policymakers."[3] The cycle has five phases: planning and direction, collection, processing, production and analysis, and dissemination (see Appendix A in Volume 2 for a depiction). As former CIA officer Arthur S. Hulnick notes, however, in the opening chapter, the idea of a "cycle" fails to capture the complexity of how intelligence is collected, assessed, and distributed by intelligence officers.

The next five chapters in Volume 2 take us into the world of the "ints," that is, the specialized "intelligences" (methods) used by intelligence officers to collect information. Patrick Radden Keefe and Matthew M. Aid probe the method of signals intelligence or SIGINT, a generic term used to describe the interception and analysis of communications intelligence and other electronic emissions, from wiretapping telephones to studying the particles emitted by missiles in test flights. Both authors are sensitive to the possible abuse of these techniques, which can be and have been used to spy on Americans without a proper judicial warrant. Jeffrey T. Richelson explores the IMINT domain, that is, imagery intelligence or, in simple terms, photographs taken by surveillance satellites and reconnaissance airplanes (piloted and unpiloted). Telephone conversations can be revealing, but

in the old saying, a picture can be worth a thousand words. (Appendix B provides photographic examples of these spy platforms, and Appendix C offers illustrations of the IMINT data they can collect.)

Important, too, is information that can be acquired by human agents ("assets") guided by case officers inside the CIA or the Defense Department, the topic of human intelligence or HUMINT, examined by Frederick P. Hitz. Not all the information needed by policy makers is acquired through SIGINT, IMINT, or HUMINT; indeed, the overwhelming majority—upward of 95 percent—is already in the public domain. This open-source intelligence (OSINT) must be sorted through, organized, and integrated with the secretly gained information. Robert David Steele's chapter looks at OSINT and its ties to the other ints.

In the next chapter, Daniel S. Gressang IV dissects some of the technological challenges faced by intelligence agencies in sorting through the avalanche of data that pours into their headquarters from various intelligence collectors around the world. Here is the Herculean task of sorting out the wheat from the chaff (or the signal from the noise, in another widely used metaphor) in the search for information that may warn the nation of impending peril. Here is the vital task of providing "indicators and warnings" (I&W) to a nation's leaders.

One of the most difficult relationships in the complex process of collection, analysis, and dissemination of information comes at the intersection between intelligence professionals and policy makers—groups of individuals that often have very different training, aspirations, and cultures. Jack Davis sheds light on this often turbulent relationship in the United States, and Michael Herman tackles the same topic in the United Kingdom. Minh A. Luong offers a case study on economic intelligence that underscores some of the difficulties encountered as information travels from the collectors and analysts (the "producers" of intelligence) to the policy makers (the "consumers"). Finally, Max M. Holland takes a look at how intelligence agencies examine their own mistakes ("postmortems") and attempt to make corrections—and how political consideration enter into the process.

By way of supporting documentation, in addition to the appendixes already mentioned, Appendix D outlines the general types of reports prepared by the producers of intelligence, along with a listing of specific examples. Appendixes E and F provide samples of key intelligence products: National Intelligence Estimates (NIEs)—the most important long-range and in-depth forecasting carried out by the U.S. secret agencies ("research intelligence," in contrast to shorter intelligence reports that tend to focus on near-term events, or "current intelligence"); Special National Intelligence Estimates (SNIEs), which concentrate on a narrow, high-priority information requirement (say, the capabilities of the Chinese military); and the *President's Daily Brief* (PDB), the most exclusive current intelligence report prepared by the intelligence agencies for the consumption of the president and a few other high-ranking officials.

In light of the fact that every study of the 9/11 and Iraqi WMD intelligence failures find fault, in part, with America's capacity for human intelligence—

especially in the Middle East and Southwest Asia—Appendix G presents one of the most searing critiques of this int. The critique, by the House Permanent Select Committee on Intelligence, has become all the more significant because the panel's chairman, Representative Porter Goss (R-FL), soon after the completion of the report rose to the position of the DCI. Last, Appendix H provides an excerpt from a key report on the Iraqi WMD mistakes, prepared by the "Roberts Committee": the Senate Select Committee on Intelligence, led by Pat Roberts (R-KS).

The third volume, titled *Covert Action: Behind the Veils of Secret Foreign Policy*, enters an especially controversial compartment of intelligence: the means by which the United States attempts to not just gather and analyze information about the world—hard enough—but to manipulate global events through secret activities in the advancement of America's best interests. An ambiguous passage of the National Security Act of 1947 charged the National Security Council (NSC), the boss over the sixteen U.S. secret agencies, to "perform such other functions and duties related to intelligence [over and beyond collection-and-analysis] affecting the national security as the National Security Council may from time to time direct."[4] The phrase "other functions and duties" left the door open for launching the CIA (and more recently the Pentagon) on a wide range of covert actions around the world.

Covert action (CA), sometimes referred to as the "quiet option," is based on the supposition that this secret approach to foreign affairs is likely to be less noisy and obtrusive than sending in the Marines. Sometimes professional practitioners also refer to covert action as the "third option," between diplomacy and open warfare. As former Secretary of State and National Security Adviser Henry Kissinger once put it: "We need an intelligence community that, in certain complicated situations, can defend the American national interest in the gray areas where military operations are not suitable and diplomacy cannot operation."[5] Still others prefer the euphemism "special activities" to describe covert action. Whatever the variation in terminology, the goal of covert action remains constant: to influence events overseas secretly and in support of American foreign policy.

Covert action operations are often grouped according to four broad categories: propaganda, political, economic, and paramilitary (PM) activities. An example of a propaganda operation was the CIA's use of Radio Free Europe during the Cold War to transmit anti-communist themes into nations behind the Iron Curtain. A political CA during the Cold War was the CIA's clandestine funneling of funds to the anti-communist Christian Democratic Party in Italy. An economic example: the CIA attempted to destroy electric power stations in Nicaragua during the 1980s, as a means of undermining the Marxist-oriented S*andinista* regime. PM operations can including everything from assassination plots against foreign heads of state to arming and guiding pro-American insurgent armies in one country or another. Little wonder this has been a controversial subject.

Gregory F. Treverton introduces the reader to covert action in the first chapter of Volume 3. He is followed by Kevin A. O'Brien and Ephraim Kahana, who discuss the use of covert action by other nations. The next four chapters illuminate certain aspects of CA, with James M. Scott and Jerel A. Rosati providing an overview of CA tradecraft (that is, the tools used to implement such operations); Michael A. Turner evaluating the merits of CIA covert propaganda operations; William J. Daugherty looking at political and economic examples of covert action; Jennifer D. Kibbe exploring the entry of the Defense Department into this domain; and former diplomat John D. Stempel contrasting the uses of covert action to diplomatic initiatives. Winding up the volume is Judge James E. Baker's legal analysis of covert action.

Supporting documents include excerpts from the Church Committee Report on the evolution of covert action as carried out by the CIA (Appendix A). The supervision of covert action went from an informal to a highly formal process, as a result of a law known as the Hughes-Ryan Act, passed on December 31, 1974. The language of this statute is presented in Appendix B, and the covert action procedures that resulted from the law are outlined in Appendix C. At the center of the covert action decision process since the Hughes-Ryan Act is the *finding*, a term of art that stems from the passage in the law that requires the president to "find" that a particular covert action proposal is important and has the president's approval. Appendix D contains two findings from the Iran-*contra* era in the mid-1980s. Covert actions must have an organizational apparatus to carry them out, and Appendix E displays what that apparatus looked like during the Cold War (and in basic form remains the organizational chart today, with a few name changes in the boxes).

One of the most controversial forms of covert action has been the assassination of foreign leaders. Appendix F presents a case study from the Church Committee on the CIA assassination plot hatched against the leader of the Republic of Congo, Patrice Lumumba, in 1960. The Committee's exposé of this and other plots led President Gerald R. Ford to sign an executive order prohibiting assassination as an instrument of American foreign policy (see Appendix G). The executive order has been waived in times of authorized warfare against other nations, however, leading to failed attempts to assassinate Saddam Hussein in the first and second Persian Gulf Wars (he was eventually captured alive in 2004, hidden away in a hole near his hometown in Iraq) and Al Qaeda leader Osama bin Laden during the Clinton administration. Considerable ambiguity exists regarding the current status of the executive order and under what conditions it might be waived by administrations. Finally, Appendix H—drawing on a presidential commission study and congressional hearings—examines covert action at its lowest state: the Iran-*contra* affair of the 1980s, when this approach to foreign policy subverted the U.S. Constitution and several laws (including the Hughes-Ryan Act).

A third intelligence mission, after collection-and-analysis and covert action, is counterintelligence (CI) and its associated activity, counterterrorism (CT).

Here is the concentration in Volume 4, titled *Counterintelligence and Counterterrorism: Defending the Nation Against Hostile Forces*. Like covert action, CI went without specific mention in the National Security Act of 1947. By the early 1950s, however, it had similarly achieved a status of considerable importance as an intelligence mission. CI specialists soon waged nothing less than a secret war against antagonistic intelligence services (especially the Soviet KGB); and, after the Cold War, CT specialists would focus on efforts to block terrorists who targeted the United States and its allies. Explaining why the mission of counterintelligence/counterterrorism evolved, a CI expert has pointed out that "in the absence of an effective U.S. counterintelligence program, [adversaries of democracy] function in what is largely a benign environment."[6]

The practice of counterintelligence consists of two matching halves: security and counterespionage. Security is the passive or defensive side of CI, involving such devices as background investigations, fences, sentries, alarms, badges, watchdogs, and polygraphs (lie detection machines). Counterespionage (CE) is the offensive or aggressive side of CI. The most effective CE operation is the infiltration of an American agent or "mole" into the enemy camp, whether a hostile intelligence service or a terrorist cell—a ploy called a penetration. Thus, the practice of security is, according to one of America's top counterintelligence experts, "All that concerns perimeter defense, badges, knowing everything you have to know about your own people," whereas the CE side "involves knowing all about intelligence services—hostile intelligence services: their people, their installations, their methods, and their operations."[7]

Stan A. Taylor and Nigel West clarify these issues in the first two chapters of this volume, then in the next two chapters Katherine A. S. Sibley and Athan Theoharis examine the challenges of keeping the United States spy-free. Rhodri Jeffreys-Jones looks at the efforts in Europe to create a counterintelligence capability similar to that practiced by America's Federal Bureau of Investigation (FBI). Glenn Hastedt takes the reader into the counterterrorism thicket in Washington, DC, explaining how politics influences CI and CT operations. Richard L. Russell and Jennifer Sims discuss the ups and downs of trying to establish an effective counterterrorism response in the United States, complicated by the fragmentation of authority and widely differing cultures among the sixteen U.S. intelligence agencies. Finally, Katharina von Knop looks at the rising role of women in terrorist organizations.

The back-of-the-book documents in Volume 4 begin with a look at the Church Committee findings regarding counterintelligence in 1975 (Appendix A), followed by the notorious Huston Plan—a master counterintelligence spy plan drafted by White House aide Tom Charles Huston in 1970, in response to a nation at unrest over the war in Vietnam (Appendix B). The Huston Plan is a classic illustration of overreaction in a time of domestic strife. In Appendix C, the Senate Select Committee on Intelligence summarizes its findings about the Aldrich H. Ames counterintelligence disaster. Next the appendixes include a series of U.S. commission conclusions about how to improve intelligence in the struggle

against global terrorism, whether locating and penetrating their cells in advance of a terrorist attack or thwarting the ability of terrorists to acquire WMDs. The panel reports include: the Hart-Rudman Commission of 2001 (Appendix D); the 9/11 or Kean Commission of 2004 (Appendix E); and the Silberman-Robb Commission of 2005 (Appendix F). For purposes of comparison, the final appendix (G) examines the conclusions reached by a British commission that also probed the Iraqi WMD failure: the Butler Report of 2004.

The fifth volume in the series, titled *Intelligence and Accountability: Safeguards Against the Abuse of Secret Power*, stems from a concern that secret power might be misused by those in high office. This danger was underscored in 1975 when Congress found the U.S. intelligence agencies guilty of spying against law-abiding American citizens, and again in 1987 during the Iran-*contra* affair when some elements of the intelligence community violated the public trust by ignoring intelligence laws. The United States has been one of the few nations in the world to conduct an ongoing experiment in bringing democratic accountability to secret government activities. Democracy and spying don't mix well. Secrecy runs counter to democratic openness, while at the same time openness possesses a threat to the success of espionage operations. Democracies need intelligence agencies to acquire information that may protect them, but thoughtful citizens worry about having secret agencies in an open society.

Until 1975, the nation's remedy for the tension between intelligence gathering and democracy was to trust the intelligence agencies and hope for the best. Elected officials treated the secret services as exceptional organizations, immune from the checks and balances envisioned by the framers of the Constitution. Lawmakers were satisfied with this arrangement, because if an operation went awry they could duck responsibility. When James R. Schlesinger, DCI in 1973, attempted to inform John Stennis (D-MS), a key member of the Senate Armed Services Committee, about an approaching operation, the Senator stopped him short: "No, no, my boy, don't tell me. Just go ahead and do it, but I don't want to know."[8]

This attitude on Capitol Hill—overlook rather than oversight—underwent a dramatic turnabout in December 1974, however, when the *New York Times* reported on allegations of CIA spying at home and questionable covert actions in Chile. Congress might have waved aside the revelations about Chile as just another Cold War necessity in the struggle against regimes leaning toward Moscow, but spying on American citizens—voters—was another matter altogether. In January 1975, President Ford created the Commission on CIA Activities Within the United States (the Rockefeller Commission, led by his vice president, Nelson Rockefeller). Later that month the Senate established a select committee to investigate intelligence activities. The committee was headed by Frank Church, D-ID, and became known as the Church Committee (the editor served as Church's assistant). A counterpart House committee, led by Representative Otis Pike (D-NY), began investigations the following month.

These various panels, especially the Church Committee, found many more improprieties than they had expected. Not only had the CIA engaged in domestic

spying in violation of its charter, so had the FBI and several military intelligence units. Furthermore, the FBI had carried out secret operations, known collectively as COINTELPRO, against thousands of civil rights activists, members of the Ku Klux Klan, and Vietnam War dissenters. The objective was to make their lives miserable by disrupting their marriages and employment. The Bureau even attempted to blackmail Dr. Martin Luther King Jr. into committing suicide. Church Committee investigators also discovered CIA assassination plots against foreign leaders and efforts to topple President Salvador Allende of Chile, even though he had been democratically elected.

These revelations convinced lawmakers that the time had come to bring accountability into the dark recesses of government. Congress established intelligence oversight committees in both chambers—the Senate in 1976 and the House a year later—and, by 1980, required by law timely reports on all secret intelligence operations. The new Committees pored over intelligence budgets, held regular hearings (mostly in closed session to protect spy sources and methods) and seriously examined the performance of America's intelligence agencies. No other nation has ever so thoroughly applied democratic principles to its secret services, although a number are now beginning to follow the leadership of the United States toward greater intelligence supervision.[9]

Since 1975, this effort has evolved in fits and starts. Sometimes lawmakers have insisted on close accountability, as when they enacted the Intelligence Oversight Act of 1980 with its stringent reporting requirements for covert operations, or when a series of laws in the 1980s sought to end covert actions in Nicaragua. At other times, members of Congress have loosened the reins—for example, repealing in 1985 a prohibition against covert action in Angola. On still other occasions, Congress has concentrated on helping the intelligence agencies improve their security and performance, as with a law in 1982 that prohibited exposing the names of undercover officers. The Iran-*contra* scandal of 1987 was a major setback to this new oversight, as the Reagan administration bypassed most of these rules and statutes in its conduct of a covert war in Nicaragua against the will of Congress. The scandal was an alert to lawmakers. The Intelligence Oversight Act of 1991 further tightened intelligence supervision by clarifying reporting requirements. Lawmakers also set up an Office of Inspector General in the CIA, confirmed by and accountable to Congress.

The pulling and tugging has continued, most recently over whether President George W. Bush violated the Foreign Intelligence Surveillance Act (FISA) of 1978 by conducting warrantless wiretaps as part of the war against terrorism in the aftermath of the 9/11 attacks. The FISA required warrants, but the White House claimed (when the secret operation leaked to the media) the law had become to cumbersome and, besides, the president had inherit authority to conduct the war against terrorism as he saw fit. This debate aside for the moment (several authors address the issue in these volumes), one thing is certain: the intelligence agencies in the United States are now very much a part of the nation's system of checks and balances. Americans want and deserve both civil liberties and a secure defense

against threats; so the search continues for an appropriate balance between liberty and security, democracy and effectiveness—precisely the topic of Volume 5.

The set of chapters on intelligence accountability are introduced with a chapter by David M. Barrett, the foremost authority on the history of accountability in the early years of modern U.S. intelligence (1947 to 1963). The chief counsel of the Church Committee, Frederick A. O. Schwarz Jr., then reflects back on the effects of that watershed inquiry. Next, the editor offers a previously unpublished interview with DCI William E. Colby, who stood at the helm of the intelligence community as it weathered the storm of the investigations into domestic spying during 1975. Mark Phythian presents a chapter on the British experience with intelligence accountability; and, comparing British and American oversight, Lawrence J. Lamanna contrasts the responses on both sides of the Atlantic to the faulty Iraqi WMD assessments in 2002.

The next chapter, written by Cynthia M. Nolan, looks at contemporary issues of intelligence oversight in the United States. Hans Born and Ian Leigh follow with a comparative dimension by contrasting intelligence accountability practices in a variety other nations. Finally, A. Denis Clift and Harry Howe Ransom, who have witnessed the unfolding of intelligence accountability over the past four decades, offer their appraisals of where the experiment stands today.

The first supporting document in this volume is a succinct legislative history of intelligence accountability from 1947 to 1993, prepared by the Senate Select Committee on Intelligence (Appendix A). Then come a series of important oversight laws, beginning with FISA in 1978. With this law, members of Congress sought to rein in the open-ended authority of the executive branch to wiretap and otherwise spy on individuals considered risks to the national security—a privilege abused by a number of administrations from the 1930s forward. Henceforth, FISA required a warrant from a special court (the FISA Court, whose members are appointed by the Chief Justice of the Supreme Court) before such intrusive measures could be carried out. This law, a hot topic in 2005–6 when critics charged the second Bush administration with violation of the warrant requirement, can be found in Appendix B.

The Intelligence Oversight Act of 1980 is presented in Appendix C. This is a brief but nonetheless far-reaching law, enacted by Congress as an attempt to become an equal partner with the executive branch when it came to intelligence. The 1991 Intelligence Oversight Act (Appendix D) emerged after the Iran-*contra* scandal and provided a tightening and clarification of the language in its 1980 precursor, especially with respect to the approval and reporting rules for covert action. The political tug-of-war over the drafting of this currently prevailing oversight statute was intense, leading to the first and only presidential veto of an intelligence act. President George H. W. Bush found the proposal's insistence on prior reporting of covert action objectionable in times of emergency. Lawmakers entered into a compromise with the chief executive, settling on a two-day reporting delay in emergencies. The bill passed Congress again, this time without a presidential veto.

In 1995, the House Permanent Select Committee on Intelligence launched an inquiry into a wide assortment of intelligence issues, stimulated initially by counterintelligence concerns (Aldrich Ames's treasonous activities at the CIA had recently been discovered) but turning into an opportunity for a broad review of new challenges that faced the secret agencies now that the Cold War had ended. In Appendix E, an excerpt from the Committee's final report examines the state of intelligence accountability in the mid-1990s. The next document, in Appendix F, carries the examination into the twenty-first century, with the appraisal of the 9/11 Commission on the same subject. The commissioners were unimpressed, referring to intelligence accountability as "dysfunctional."

At the center of any efforts to maintain accountability for the secret agencies lies the question of funding—the mighty power of the pursue, held in the hands of lawmakers. Appendix G draws on the findings of the Aspin-Brown Commission to provide official documentation about how the United States spends money for spying. Finally, in Appendix H, DCI Robert M. Gates (1991–93) offers observations about oversight from the perspective of the intelligence community management team, located at that time on the Seventh Floor of the CIA.

Here, then, is what the reader will find in these five volumes. The editor and the contributors hope the chapters and documents will help educate the public about the importance of intelligence agencies, as well as stimulate scholars around the world to further the blossoming of this vital field of study. I am pleased to acknowledge my gratitude to Praeger's Heather Staines, senior project editor, and Anne Rehill, development editor, each a pleasure to work with and most helpful in their guidance; Julie Maynard at the University of Georgia for her administrative assistance; Lawrence J. Lamanna, my graduate research assistant, for his good counsel and logistical help; Leena S. Johnson for her indispensable encouragement and support; and the contributors to these volumes for their outstanding scholarship and their much appreciated cooperation in keeping the publishing train running on time.

These volumes are enthusiastically dedicated to Harry Howe Ransom, who has done so much in the United States to lead the way toward a serious discipline of intelligence studies.

Loch K. Johnson

NOTES

1. Some of the authors have had multiple careers, so in categorizing them I have counted the place where they have spent most of their professional lives.

2. Quoted by Senator Frank Church (D-ID), in *Congressional Record* (January 27, 1976), p. 1165.

3. *Fact Book on Intelligence* (Washington DC: CIA Office of Public Affairs, April 1983), p. 17.

4. National Security Act of 1947, signed on July 26, 1947 (P.L. 97-222; 50 U.S.C. 403, Sec. 102).

5. Comment, "Evening News," NBC (January 13, 1978).

6. Editor's interview with a FBI counterintelligence specialist, Washington, DC (May 16, 1975).

7. Editor's interview with Raymond Rocca, CIA/CI specialist, Washington, DC (November 23, 1975).

8. Editor's interview with James R. Schlesinger, Washington, DC (June 16, 1994).

9. See Hans Born, Loch K. Johnson, and Ian Leigh, *Who's Watching the Spies? Establishing Intelligence Service Accountability* (Washington, DC: Potomac Books, 2005).

1

WHAT'S WRONG WITH THE INTELLIGENCE CYCLE?

ARTHUR S. HULNICK

NO CONCEPT IS MORE DEEPLY ENSHRINED IN the literature than that of the "intelligence cycle." Readers can see this clearly from the other chapters in this volume. I studied the intelligence cycle as an undergraduate in Sherman Kent's book on strategic intelligence and then later when I attended the U.S. Air Force Intelligence School in 1957.[1] In 1965, in the training courses required by the Central Intelligence Agency (CIA), I studied it yet again. When it came time to start writing about intelligence, a practice I began in my later years in the CIA, I realized that there were serious problems with the intelligence cycle.[2] It is really not a very good description of the ways in which the intelligence process works. Additionally, it ignores two main parts of intelligence work, counterintelligence and covert action. There is an alternative view.

THE FIRST STEP

The intelligence cycle is so nicely described in other chapters that there seems no need to go over it here. So, let us start at the beginning and look at what is wrong. The notion that policy makers, or intelligence consumers, as they are sometimes called, provide guidance to intelligence managers to begin the intelligence process is incorrect. Policy consumers do sometimes indicate their main concerns to intelligence managers, but often they assume that the intelligence system will alert them to problems, or provide judgments about the future. Consumers will sometimes tell intelligence managers what they are worried about, or the direction in which they intend to take policy—but not always.

Still, it is usually not too difficult for intelligence managers to learn what policy makers are up to, but the managers often have to take the initiative to obtain the information. If intelligence managers at various levels are in touch with their policy counterparts, this sharing of information may work quite well. Over the years, intelligence managers have tried to systematize this process by asking policy officials to provide specifics on their concerns. In the Carter administration, for example, a system of National Intelligence Topics (NITs) was created as a way of soliciting guidance for intelligence. Later, they were called Key Intelligence Questions (KIQs). In some cases, when policy consumers failed to submit NITs or KIQs, managers had to resort to sending policy officials a list of topics, asking them to cross out the ones they thought were not necessary, or adding those they wanted to add to the list. Even then, the lists were sometimes ignored.

In the end, intelligence managers have to make decisions about the subjects that ought to be covered. Often, this is driven by world events. But, none of this provides guidance for intelligence collection. The guidance comes from within the system. Secretary of Defense Donald Rumsfeld, in the George W. Bush administration, is reported to have once said that "we don't know what we don't know," but that is usually not the case. Intelligence managers often know what gaps exist in the intelligence data base, derived from intelligence collectors, and analysts. Filling the gaps is what drives the intelligence collection process, not guidance from policy makers. Thus, the first step in the intelligence cycle is incorrect in reality.

THE SECOND STEP

The second step is equally incorrect. Collection managers cannot wait for guidance in regard to gaps in the intelligence data base to begin the collection process. The gaps will be filled once the collection process is under way. For example, in running espionage operations, commonly called HUMINT (for human intelligence), it may take months or years to find a person who has access to the information needed and is willing to be recruited as a spy. The same may be true for technical collection sensors. Satellites in space, which make up many of the sensor platforms, are not nearly as flexible as managers would wish. Thus, anticipating the intended targets cannot be overlooked. For example, during the British confrontation with Argentina over the Falkland Islands, the United States could not help the British with space imagery because the satellite, programmed to observe the Soviet Union at that time, only passed over the Falklands at night.

Of course, with the use of unmanned aerial vehicles, imagery collection has become more easily refocused on targets of opportunity, but the unmanned aircraft may still not be in the right place when they are needed. Even open source intelligence (OSINT), which has been given new life in recent years because of the proliferation of information on the Internet, requires planning to ensure access to needed material. Intelligence managers need sophisticated software to mine the data because there is so much of it.

THE REAL DRIVERS

For all these reasons, intelligence managers, and not policy officials, are the real drivers of the intelligence collection process. Clearly, intelligence moves from collection to analysis, as the intelligence cycle holds, but analysts do not always need new intelligence material to understand world events. The data base is already so large that a competent analyst could write about most events without any more than open sources to spur the process. The incremental addition of new intelligence from human sources or technical sensors may modify the analytic process but rarely drives it.

The job of the analyst is, in part, to evaluate raw material and put it in perspective. The analyst receives intelligence material from a variety of sources, including media reports, official reports from other government agencies, as well as reports from the intelligence collection process. In my experience as a practicing analyst in the military and in the CIA, raw reports from human sources or technical sensors are sometimes fragmentary, biased, contradictory, or just plain wrong. In order to analyze the data, the analyst compares the new material with the existing data base and previous analysis. Hanging a finished product—whether it is current reporting or a longer range estimate—on one source usually does not work well. This is apparently what happened in the case of the estimate on weapons of mass destruction (WMD) in Iraq that helped trigger the invasion of that country. The estimate was based, in part, on the reporting of one rather poor and unreliable source. The estimate turned out to be quite wrong, as we now know.[3]

OPERATING IN PARALLEL

A better way of looking at the relationship of intelligence collection and intelligence analysis is to think of the two processes as operating in parallel rather than sequentially. The two processes are co-equal in terms of utility. It is important to note as well that raw reporting from the collection process, set up into standardized formats, usually goes to policy officials as well as to analysts at about the same time. Though this may not always be true in other intelligence systems, it is certainly true in the United States. Whereas senior policy officials may not see a great deal of the raw reporting, there are usually watch centers at the various policy agencies that screen the raw reporting and send forward the most interesting ones.

Unfortunately, as I have already noted, some of this raw intelligence may be incomplete, contradictory, or just wrong. Policy officials sometimes take the reporting as having been judged and evaluated. Thus, I have heard officials say that the CIA has reported an event, when in fact what the officials have seen is an unevaluated agent report passed along to them by their watch centers. It is not possible to stop this flow of raw reporting. As Bob Gates, the former Director of the CIA once noted to me, once the spigot is opened, it is not possible to close it,

even though allowing consumers to have raw reporting at about the same time as the analysts receive them creates some serious problems for the analysts. Collection managers often take a different view. They believe they are doing a great service to the policy community by providing this raw reporting. If the intelligence cycle really worked, the circulation of raw reports to policy officials would not happen.

A MAJOR PROBLEM

Since intelligence collection and intelligence analysis operate in parallel and should be co-equal, one would expect that there would be a great deal of information sharing between the two. Regrettably, this is not always the case. Because of restrictions of information sharing, psychological barriers, fears of compromising sources, and security concerns, the intelligence collection process and the intelligence analytic process not only operate in parallel, they are sometimes quite independent of each other. This is a major problem.

When I first joined the CIA, I was assigned on a temporary basis to an office in the Directorate of Plans (DDP), later renamed the Directorate of Operations (DO), and in 2005, renamed yet again as the National Clandestine Service (NCS). My job was to deal with incoming reports from the field. When an interesting report came in one day, I asked my boss if we should alert the relevant analyst about it. He rejected the idea, saying that our job was to send reports like it to the White House, and not to the Directorate of Intelligence, since analysts were not worth the attention. I was shocked. Later, when I became an analyst, I did my best to establish good relations with my operational colleagues, but there were issues.

BARRIERS TO COMMUNICATION

In those days there were physical barriers, manned by armed guards, to prevent analysts and operations officers from visiting each other's offices. Later, the physical barriers were removed, but the psychological ones remained. Operations people feared that somehow analysts would mishandle reports from the field and reveal the identity of clandestine sources. Analysts mistrusted operations officers because they were thought to be devious and untrustworthy. This mistrust was kindled in part because analysts in those days tended to be introverts who found the extroverted personality of the typical operations officers to be abrasive. Operations people tended to think that the introverted analysts were "wimps."

Over the years these stereotypes have largely been overcome, but recent efforts to increase communication between analysts and operators by colocating them have not always been successful. Agency managers have pushed analysts to take tours overseas with field stations, but it is more difficult for an operations

officer to serve a tour as an analyst. Similar issues may not arise in other intelligence agencies unless they have co-equal collection and analysis components.

The Defense Intelligence Agency (DIA), for example, was immune to this sort of "stovepipe" problem because it was mostly an analytic rather than collection agency. As Defense HUMINT grows, perhaps the same problem will arise. The National Security Agency (NSA) and the National Geo-Spatial Intelligence Agencies (NGIA) are devoted mostly to collection, but they tend to be tightly compartmentalized, creating a different kind of "stovepipe" problem. In theory, all the intelligence agencies should share raw data and coordinate analysis, but for a variety of reasons they do not always do so. This was one of the main critiques of both the 9/11 Commission and the commission investigating the intelligence failure surrounding the estimate on WMD.

A MIXED BAG

There is a tendency among intelligence agencies to hold back the most sensitive and exciting reports until the agency's leaders have been able to deliver the reports to senior policy officials, thus highlighting the skill and cleverness of their people and "scoring points" with the officials. One effort to spur interagency communications has been the establishment of centers, where all the agencies have representation and where their representatives can easily talk with their counterparts, even informally, to discuss events and incoming intelligence. The establishment of these centers has been something of a mixed bag. We know from the 9/11 investigations that the then-existing counterterrorism center (CTC) was not a place where all information was shared.[4]

Now, efforts at intelligence reform have "morphed" the CTC into a National Counterterrorism Center (NCTC), controlled by the new Director of National Intelligence (DNI). Will that spur the agencies into more easily sharing their best and most sensitive data? It would be nice to think so, but experience shows that this does not always happen, even at the highest level.

THE FINAL STAGES

In the final stages of the intelligence cycle finished intelligence, broken down into a variety of products, emerges from the analytic process. It is supposed to be delivered to policy officials—the literature refers to this delivery as dissemination—and then policy officials either make decisions or create further requirements and the cycle starts over again. This, too, is a distortion of what really happens. Much of this depends on the kind of intelligence product that is being delivered. These products include warning intelligence, in which consumers are alerted to "breaking news," current intelligence to update consumers on world events on which they already have some knowledge, in-depth studies on

particular situations or issues, and forecasts of the future, the estimate. All products are received and used in a different way, but none of them really drive the policy process.

Warning intelligence is supposed to alert policy officials to breaking world situations, especially those for which they may have to take action. Both intelligence managers and policy consumers hate surprise. It is embarrassing for intelligence when the system misses an event about which it should have had information. For example, the CIA failed to detect the fact that the Indian government planned to conduct a nuclear test in 1998. Later investigations revealed that this was both a collection and an analysis failure. The CIA had no assets it could tap in India at that time, and the Indian analyst at the CIA had somehow missed the fact that the Indian prime minister had declared his intention to hold the tests. Despite the fact that there was little the U.S. government could do to stop the tests, policy officials were nonetheless outraged at this failure.[5]

Even greater outrage was directed at the entire intelligence community for its failure to detect the 9/11 terrorist attack on the United States. This has been exhaustively examined and has led to the restructuring of the intelligence system. Yet, there is considerable evidence that there was little that might have been done to avert the disaster. But, it illustrates the point that policy officials expect the intelligence system to be all-knowing, all-seeing, and always correct. As Richard Betts pointed out many years ago, intelligence failure is probably inevitable.[6]

Warning of crisis should come early enough so that policy officials can have time to develop some kind of considered response. Unfortunately, the warning may come so late that it is really an alert that the crisis has already begun. Using a system that is composed of warning centers at major military commands, tied in to warning centers at all the intelligence agencies and in policy departments in Washington, and taking advantage of the proliferation of twenty-four-hour TV and Internet outlets, the warning network rarely misses the start of a crisis, and it is then able to reach out to decision makers quite rapidly. When the decision makers ask intelligence officers how they should respond to the crisis, typically intelligence officers decline to provide advice, thus staying clear of the policy process.

THE MOST USEFUL PRODUCT

Current or daily intelligence is the most ubiquitous of all types of intelligence products, delivered at all levels and usually first thing in the morning. It is designed to supplement the media, based on the assumption that policy officials have already gotten their media inputs from newspapers or television news. It is the most popular of all intelligence products because current intelligence is an "easy read," short, and to the point. For those policy officials who only have ten or fifteen minutes a day to absorb intelligence products—and consumer surveys consistently show that this is about all the time policy officials have for such

things—current intelligence is rated as the most useful product from the intelligence community. The idea of this product is to summarize events, explain how they fit into some context, and suggest what might happen next. It is a very journalistic methodology.

Unlike warning intelligence that may lead to policy action, as the intelligence cycle suggests, current intelligence hardly ever leads to policy decisions—and it is not meant to do so. Instead, it gives generalists at senior levels a chance to find out about events outside their main areas of responsibility. Specialists often complain that the daily intelligence flow does not provide the level of detail they would need to make policy, but the current intelligence products are not designed for specialists. In fact, it would be quite likely that specialists would have seen a great deal of the raw intelligence data that lay behind the current intelligence product anyway.

During the 9/11 investigation, much was made of the fact that one daily publication, the *President's Daily Brief* (PDB), had on August 6, 2001, reported the possibility that terrorists might use commercial aircraft as cruise missiles to attack commercial or government buildings within the United States.[7] Critics of the president took this to have been a warning the president and his senior staff had missed, but normally the PDB would not have been the kind of intelligence product used for warning. The warning would have been delivered in a much more specific document devoted entirely to the subject. Intelligence managers have never expected the PDB or similar publications to be more than educational in nature. Certainly, these publications do not drive the intelligence process.

IN-DEPTH STUDIES

The same might be said for the myriad in-depth intelligence studies churned out by the analytic components. These studies have proliferated in recent years, although they were rarely attempted at the beginning of the Cold War. These studies are designed to provide in-depth analysis on specific subjects and are meant more for policy officials at working levels rather than senior decision makers, who rarely have the time to read them. These studies help in forcing analysts to come to grips with a specific subject, provide useful information to consumers within the intelligence system, and support policy makers as they design policy initiatives.

The production of these studies grew over the years as a way of giving analysts a vehicle for attacking a problem in more depth than was possible in a daily or weekly publication, and without the fuss and bureaucracy involved in producing the more formal national estimate. Policy officials sometimes request these in-depth studies, along the lines suggested by some versions of the intelligence cycle, but in many cases, the studies are produced because analysts are directed by intelligence managers to write them, or analysts themselves believe they should be written. When Robert M. Gates took over the Directorate of

Intelligence (DI) at the CIA during the early days of the Reagan administration, he decreed that analysts should produce at least two of these in-depth studies every year. Gates was fond of pointing out that the DI produced about 5,000 of these studies one year. It was not clear, however, how many of them were actually read.

In recent years, these studies have been more carefully tailored to the needs of policy officials. The same might be said for the Defense Intelligence Agency products, which are geared to military needs, or those coming from the State Department's intelligence and research unit, which has always focused its analysis on foreign policy issues. The fourth category of product, the estimate, is the one most likely to drive the policy process, at least in theory. But the reality is often different.

THE REALITY OF ESTIMATES

The estimate is a creature of the Cold War, it but has its roots in World War II. It is supposed to be a forecast of the future that decision makers can use to build policy, just as the intelligence cycle proposes. The estimate is supposed to be drawn by analysts from all the producing agencies, coordinated by the analysts among themselves to reach an agreed forecast, with dissenting views included. Then, it is blessed by the agency leaders; is signed off at the top; is sent to the president, the National Security Council, and staffs; and serves as the basis for policy discussions. There are actually cases where this has happened, where decision makers have waited for the intelligence community's views as embodied in the estimate, but these cases are rare.

The reality is that policy officials often know what they want to do even before they receive the estimate and hope that this product will confirm in some way the wisdom of the path they have already chosen. When the estimate conflicts with their views, policy consumers may dismiss it as uninformed, useless, or even obstructionist. When it agrees with what they think they already know, then they may see it as confirming, irrelevant, or again useless. Although one would think that policy makers would want to know when they were heading in the wrong direction, this is not usually the case. Policy consumers do not welcome intelligence that is nonconfirming, perhaps because the large egos that brought them into positions of power do not permit admissions of ignorance.

THE WMD CASE

There is no better example of what can go wrong in the estimates process than the recent experience with the problems related to Iraq and Saddam Hussein's alleged possession of weapons of mass destruction. We now know how the

intelligence system politicized the estimate to meet the needs of the George W. Bush administration. The estimate on WMD was flawed from the beginning. It was based on the reporting of only a few unreliable sources. Then, analysts made several faulty assumptions about the weapons Saddam Hussein had had or used before the first Gulf War. Finally, policy officials used the estimate to convince both Americans and other nations that Saddam was about to develop nuclear weapons. All of this was wrong.[8]

According to James Risen, intelligence officials in both the collection and analysis arms of the CIA, as well as those in other agencies, knew the sources were poor and the conclusions wrong, but they could not fight senior managers who wanted to satisfy the political needs of the White House. Even more corrupting, it appears that Secretary of Defense Rumsfeld, fearing that the estimate would not support the already planned invasion of Iraq, sent his own officials, neither of them intelligence officers, to find the "correct" information.[9] All these steps were perversions of the estimates process. One can only hope that such antics will not take place in the future.

For all the reasons cited, it seems clear to me that trying to learn how intelligence works by using the intelligence cycle model will lead to misunderstandings about what really happens in the intelligence world. Collection and analysis are really parallel processes. The key to their effective functioning lies in the extent to which there is good communication between the two processes. There needs to be, as well, good communication between intelligence managers and policy consumers throughout the intelligence process. At the same time, however, intelligence managers must stand up to policy officials when they seek to make the intelligence judgments conform to political needs.

INTELLIGENCE AND POLICY

In the early days of the Cold War, the founders of the CIA debated the extent to which intelligence should be close to policy. Sherman Kent, a Yale professor who went on to establish the national estimates system in the CIA, and one of the early thinkers about the intelligence process, believed as did "Wild Bill" Donovan and others, that if intelligence became enmeshed in the policy process, it would lose its value. Kent argued that the best way to avoid politicization of intelligence was to remain distant and aloof. Later, Roger Hilsman, one of the intelligence chiefs at the State Department, took a different view. Hilsman thought that intelligence had to be close to policy to remain relevant.[10] The experiences of the Bush era suggest that Kent may have been right all along.

Nonetheless, other studies have shown that there must be good communication between policy consumers and intelligence managers if intelligence is to be on target and meet the needs of decision makers. At the same time, intelligence managers have to stand up to efforts by policy officials to skew intelligence

judgments when the conclusions are at variance with the political proclivities of partisan officials. No one said this would be easy. It is a constant challenge to provide "truth to power." Intelligence must deliver the unvarnished bottom line. Policy officials can go elsewhere for politicized information if they wish, but at their own peril.

LOOKING AT COUNTERINTELLIGENCE

Leaving aside the collection and analysis processes in intelligence, one cannot understand the entire intelligence system without looking at counterintelligence. Counterintelligence is largely defensive in nature, and it is not part of the traditional intelligence cycle—although some writers have tried to adapt the cycle into a counterintelligence model.[11] In my view, counterintelligence follows an entirely different and unique path, with a model of its own. It is certainly worth studying because counterintelligence is a major function of intelligence, consists of both active and passive components, and has become as controversial as any aspect of the intelligence function in government.

In its earliest forms, counterintelligence usually meant counterespionage, stopping enemy, adversary, or even friendly spies from stealing a country's own secrets. Of course, the target country might very well be carrying out espionage against the enemies, adversaries, or friends at the same time as it tries to defend against similar sorts of spying. Thus, stealing secrets for one's country is good and necessary; having one's secrets stolen is dangerous and despicable. U.S. intelligence officers, for example, are rewarded for their successes in gathering information from their targets, even though some of what they do may be illegal in the countries they target. At the same time, other U.S. intelligence officers are heralded for their ability to root out foreign spies and are castigated when they fail to do so. After all, espionage is illegal in the United States and must be stopped.

MORE DIVERSE

Today, counterintelligence has become much more diverse than just stopping spies. It now means countering terrorism, narcotics flows, global organized crime, and subversion. Whatever the threat, however, the patterns of intelligence activity in fighting all of them are similar. It has nothing to do with the intelligence cycle. Instead, there is a counterintelligence methodology that is unique.

First, in countering national security threats, counterintelligence units must identify and locate the evil-doers. This might be foreign intelligence operatives working for a hostile intelligence service, a terrorist cell, a unit of a crime "army," or a group of narcotics pushers. There are several proven intelligence methods for identifying the "bad guys," including the use of: penetrations, or "moles," to get

on the inside of the groups or services; surveillance, either physical or technical; informants; and intelligence derived from captured or detained individuals. All have both positive and negative aspects.

Based on the Cold War experience, we know that it is possible to recruit officials of a foreign intelligence service to turn coat and betray some of the activities of their operatives. There are several known cases where the United States was able to place a mole inside a foreign service, and there were a number of U.S. intelligence officers—such as Aldrich Ames, John Walker, and Robert Hanssen—who gave away U.S. secrets to the Soviets. The FBI seemed quite capable of recruiting penetrations of crime groups such as the Sicilian Mafia. Penetrating a terrorist cell is far more difficult and dangerous. Terrorist cells are usually made up of a handful of people, all of whom may be bonded by family or religious ties. Even if a terrorist cell member wanted to become a "double agent," the first hint of disloyalty to the cell could result in death.

Physical or electronic surveillance is another proven method of identifying counterintelligence targets. Overseas, this kind of surveillance can be mounted against potential targets as a result of decisions by intelligence managers. In the United States, however, the rules are more strict. Counterintelligence officials would, in most circumstances, be required to go through a legal process and obtain a warrant before employing surveillance against a U.S. citizen, a resident alien, or a U.S. person. This issue became frontpage news early in 2006 when the *New York Times* revealed that President George W. Bush had authorized surveillance of communications without warrant, arguing that Congress had given the president the authority to do so.[12] The issue may not be resolved until a court case is brought, or new legislation is passed defining the parameters of surveillance use domestically.

USING INFORMANTS

Informants can be very useful in identifying counterintelligence targets. Informants are not recruited agents, but rather people who see something amiss and report their suspicions to authorities. In hostage situations, informants may be able to point out where unusual activity is taking place. For example, prior to 9/11, flight school managers reported to the Federal Bureau of Investigation (FBI) their concerns about Middle Eastern men seeking flight training only to steer aircraft, rather than learn to take off and land. Unfortunately, FBI senior officials refused to grant field agents permission to interview the informants, claiming that there was no probable cause to do so.[13]

Informants can also cause a lot of wasted effort. During the sniper crisis in Washington, DC, in 2002, in which two men were able to terrorize the area by random attacks on innocent targets, requests for information resulted in more than 100,000 inputs, of which 40,000 were worth investigating.[14] People who have experience in fielding informant reports note that often the reports are used to

denounce spouses, parents, or unpleasant neighbors, and provide no useful intelligence. Nonetheless, informants can prove to be helpful in identifying bad guys.

INTELLIGENCE FROM INTERROGATION

After 9/11 a good deal of controversy arose over the use of intelligence gained from the interrogation of detainees, either overseas or here at home. In the wake of 9/11 some men of Middle Eastern Muslim extraction, who were not U.S. citizens, were required to register with the federal government. Some of these people had irregularities in their visas, had overstayed their stay in the United States, or were in the United States illegally. They were detained in somewhat harsh conditions and in some cases, badly mistreated. It did not appear, however, that much effort was made to find out if any of them had ties to terrorism.

At the same time, as the United States geared up to take down the Taliban government in Afghanistan, some Taliban fighters or people associated with Al Qaeda were captured, turned in by informants, or sold to the United States, by Afghan warlords. These people, dubbed "enemy combatants" by the Bush administration, were shipped to the Guantanamo Naval Base in Cuba, where U.S. authorities said U.S. legal rules did not apply to them. These people were interrogated using what some described as harsh methods, or even torture, according to press reports.

After the United States invaded Iraq in 2003, more detainees were captured on the battlefield. These fighters were imprisoned in Iraq at some of Saddam Hussein's former prisons, including the infamous one at Abu Ghraib. It was at this location that the worst abuses took place. Apparently, unschooled, unscreened, untrained guards were turned loose to abuse the prisoners in the mistaken belief that this would "soften them up" for interrogation. All of these situations involving detainees were handled badly.

Long experience has taught that there are effective ways to interrogate prisoners, using methods that do no harm to the subjects while producing useful intelligence. Unfortunately, those lessons were not applied effectively in the post-9/11 situations. The literature on interrogation methods, on training interrogators, on handling subjects should have been readily available to anyone involved in trying to extract intelligence from detainees. Anyone who has been involved in intelligence style interrogations knows that torture is ineffective and counterproductive, as well as abhorrent and illegal. Since those experiences, the rules have been changed to exclude such behavior by U.S. officials.

A good interrogation may yield only bits and pieces of information, but if intelligence collectors are careful, they may be able to piece together a broader picture from a series of subjects. The main aim, of course, is to try to learn something about the cells, or units, that the subjects have come from, especially about their plans for future operations.

STOPPING THE BAD GUYS

After the "bad guys" have been identified, then a decision has to be made about the kinds of operations that will be mounted to stop whatever kind of plan or activity might be under way against U.S. interests. This creates a dilemma. Usually, intelligence officers will press to extend or broaden the collection effort to make sure that all the bad guys have been identified and located. At the same time, law enforcement officials are eager to bring the bad guys to justice. This creates a serious problem, often described as the "cops and spies" dilemma.[15]

The divisions between law enforcement and intelligence in the United States have deep roots. Unlike many other industrialized countries, the United States does not have a domestic intelligence service, such as the MI-5 in Great Britain, or the DST in France. Instead, the United States has relied for many years on the FBI—which is really a law enforcement organization—to gather counterintelligence and then act to bring lawbreakers to justice. In other countries, the domestic intelligence services collect and analyze counterintelligence in parallel with counterpart foreign intelligence organizations, which work beyond the country's borders. When suspected criminal behavior is uncovered, the domestic intelligence services may turn to national police organizations to carry out law enforcement operations against the suspects.

INTELLIGENCE VERSUS LAW ENFORCEMENT

In the United States, however, where no domestic intelligence service has existed, there have been both legal and procedural barriers between the national intelligence services, whose focus has been almost exclusively abroad, and the FBI, which has always had a role in domestic counterintelligence. Traditionally, counterintelligence collected abroad was passed to the FBI, which then determined, usually in consultation with the Justice Department, whether there was probable cause to open a criminal investigation. This would be used to gather evidence that could be brought if a court case arose. This was different from the gathering and analysis of intelligence data, which traditionally was not treated or handled as evidence.

Because of cover considerations and the need to protect the identity of intelligence officers, intelligence managers did not want their people to have to appear in court, and wanted as well to protect the sources and methods used to collect intelligence. The FBI was under no such strictures, but the evidence they gathered had to be backed by appropriate warrants and protected according to legal standards. The Aldrich Ames case is a perfect example of how this system used to work.

A joint CIA and FBI team was able to track down Ames and identify him as a Soviet mole in the CIA. Then, the FBI obtained a warrant under the Foreign Intelligence Surveillance Act (FISA) to be certain that they had the right target.

Once that was done, a second FBI team, with a criminal warrant, took over the investigation and gathered evidence that might be used to prosecute Ames. In the end, Ames agreed to a plea bargain and the case never came to court, but it illustrates how a firewall was in place to separate the counterintelligence investigation from the criminal one.[16]

TAKING DOWN BARRIERS

Since 9/11 some of the barriers between intelligence and law enforcement have been weakened, but the cops and spies dilemma still exists. Under the new rules, the FBI may levy requirements on the U.S. intelligence services to collect information specific to their domestic needs. It is not yet clear if such intelligence would be used as evidence in court cases. More likely, the FBI would ask that intelligence be gathered to support its newly created National Security Branch, which combines the FBI's older counterterrorism and counterintelligence units with its newer intelligence bureau, created after 9/11.

At the same time, the CIA and the FBI have drawn more closely together with a strong push from Congress. FBI agents have been assigned to the CIA for counterintelligence purposes for many years, and more recently, to fight terrorism. CIA officers are reportedly working closely with FBI field offices where antiterrorism task forces have been created. While this may break down traditional barriers between the two agencies, there is still some resentment among CIA officers about the growing role of FBI attachés serving abroad, and FBI concerns about the reluctance of CIA officers to share information.

THE COUNTERINTELLIGENCE MODEL

So, when one looks at the pattern of counterintelligence functions, it does not look at all like the intelligence cycle. Instead, it may be seen as follows:

IDENTIFICATION
PENETRATION
EXPLOITATION
INTERDICTION
CLAIM SUCCESS

In this pattern, exploitation is the process of learning as much as possible about the bad guys before moving against them. Interdiction means either arresting the law breakers or pre-empting their operations. Though political leaders often talk about bringing the enemy to justice, suggesting that they would be arrested and taken to trial, convicted, and punished in the fight against terrorism, pre-emption may be the preferred course of action, especially overseas. In one

case, for example, a U.S. *Predator* with a missile on board was reportedly used to strike a terrorist leader in Yemen, killing him and his associates while they were driving in the desert.[17] One might argue that this was punishment before trial, or alternatively, that this was necessary to prevent the terrorist from leading a strike against the United States.

The downside of pre-emption is that sometimes innocent victims are slain along with the intended targets. That was apparently what happened when the Bush administration launched a missile from a drone aircraft against Ayman al-Zawahiri, Osama bin Laden's deputy, early in 2006. The missile killed 17 people, according to press reports, but not the intended target, who later broadcast an attack on Mr. Bush, equating him with Adolf Hitler. Despite the failure to kill Zawahiri, the Bush administration later said that the attack had indeed killed an important terrorist leader and was worth the cost.[18]

EXPLOITATION BEFORE INTERDICTION

In the counterintelligence model, exploitation comes before interdiction, meaning that as much intelligence should be gathered before the case or operation is turned over to law enforcement. Of course, in cases in which there is pressure to stop the enemy or adversary, exploitation may come before the intelligence is fully gathered. For example, in the case of the "Lackawanna Six," exploitation was cut short because of the need for political leaders to show that they were cracking down on terrorism. The Six were Yemeni immigrants living outside Buffalo, New York, who went to Afghanistan before 9/11 in the misguided belief that training with the Talilban fighters was going to be something of a lark.[19]

When they discovered that the Taliban were really training terrorists, the Yemeni immigrants returned to the United States. After 9/11, they turned themselves in to authorities to explain what they had done. They were quickly arrested, and eventually jailed. No one at the time seemed to realize that at least one or two of them might have been sent back to Afghanistan as double agents to penetrate Al Qaeda. Even an effort to learn more about their experiences was cut short by the pressure to achieve quick convictions to show that the government was moving swiftly against terrorism.

CLAIMING SUCCESS

Finally, in the last step of the counterintelligence process, authorities often make public claims of success, a rare step in intelligence work. Normally, intelligence managers try very hard to keep successes secret so that they might be repeated. An oft-quoted CIA saying is, "The secret of our success is the secret of our success."[20] In cases in which intelligence has been gathered successfully,

it is critical to protect sources and methods. In counterintelligence, however, the claim of success, made when the case has ended, could be used to convince the public that the government is ever watchful and actually doing something with the billions of dollars spent on intelligence. During his tenure as FBI director, J. Edgar Hoover made a fine art out of going public with counterintelligence success. His senior agents all received training in public relations and the FBI was made to look good, even when serious mistakes had been made.[21]

Whereas intelligence is usually carefully hidden (except for the counterintelligence cases), intelligence failure quickly becomes public. This is a serious problem for intelligence managers. In the early days of the CIA there was no public affairs function even to deal with the public or the media. When Admiral Turner became director, however, he instituted a Public Affairs Office, much to the chagrin of many old-timers. Since then, the CIA has had to wrestle with the appropriate response when media queries arise. This is especially true when a spy case, such as the capture of Aldrich Ames, becomes public knowledge, or when a covert action surfaces.

More forthcoming CIA directors, such as George Tenet, have had the Public Affairs Office respond generously to media questions. Under the successor regime of Porter Goss as CIA director, however, the CIA seemed to return to a more conservative approach. In such cases, it would not be uncommon for the media to receive the standard answer to questions about intelligence. This says that the CIA "can neither confirm nor deny allegations of intelligence activity," which is little more forthcoming than "no comment." Nonetheless, enterprising reporters, such as Bill Gertz of the *Washington Times* and James Risen of the *New York Times*, seem to be quite successful in learning about inside stories at the CIA and other intelligence agencies.

DEFENSIVE COUNTER INTELLIGENCE

There are defensive measures in counterintelligence that do not fit into either the traditional intelligence cycle or the model just described. These measures are often lumped together as various aspects of security. They include careful background checks on prospective employees, including the use of polygraph interviews to verify the information candidates submit on their applications, and continuing monitoring of employees throughout their careers. Facilities used for intelligence and other governmental functions are extensively guarded and patrolled, monitored with alarm and surveillance devices, and protected by barrier entry devices to keep out unwanted visitors.

Some facilities have protective systems in roadways and parking areas that can be activated to stop suicidal vehicle bombers. Buildings may be shielded electronically to prevent an adversary's use of listening devices or electronic surveillance to intercept and steal secrets. Most important, employees are trained in security awareness, so that they can report anything that seems to be a threat.

They are taught to protect the secrets with which they have been entrusted, and this responsibility lasts even after they leave their employment.

For example, those of us who were once inside the system and signed secrecy agreements are obligated to submit their published materials, including this chapter, to their agencies for review before they are given to their editors and publishers. This is not censorship, but rather a system to ensure that no secret information is inadvertently released. Some CIA authors have taken advantage of this system to include blacked-out passages in their books, demonstrating that they really were prepared to release sensitive information but were stopped by the review process. This tends to sell more books and can be a clever marketing ploy.

THE COVERT ACTION FUNCTION

The last function of intelligence—and again one not included in the intelligence cycle—is that of covert action, or special operations. This activity is not really intelligence in its traditional role of gathering and analyzing information, but rather the use of intelligence resources to carry out the national security policy of the state using surreptitious methods. Intelligence agencies around the globe carry out such operations because they have the necessary secret facilities and personnel. All through the Cold War, it was covert action that drew most of the attention and most of the criticism of American intelligence.

General Jimmy Doolittle, one of the notable heroes of World War II, after taking a hard look at intelligence in the immediate postwar period, concluded that the United States would have to be more clever, more tricky, and more devious than our Communist adversaries if we were to overcome their bid for world domination. He stated that Americans would just have to accept this "repugnant" policy.[22] When the CIA became involved in trying to overthrow governments in Guatemala, Iran, Indonesia, and Cuba, and was severely criticized in some quarters for having done so, it became clear that there were limits to what the American people were prepared to accept.

Much has been written about the nature and limits of covert action, and there seems no need to repeat that here.[23] Though covert action does not fit into the intelligence cycle, there is a pattern to this function worth outlining. This pattern is similar to other aspects of policy development and implementation, except that covert action is supposed to be secret and to disguise the role of the United States.

POLICY FORMULATION

The pattern of policy formulation looks a bit like the intelligence cycle, but in reality it is quite different. In the first step of the policy process policy officials

within the national security bureaucracy recognize and identify a problem they must address. Theoretically, the identification of the problem comes from intelligence, but in reality policy officials often see this at about the same time as intelligence officials because both receive the incoming data at about the same time, as explained earlier.

In the next step policy officials begin to seek options for dealing with the problem, assuming some role for the United States is necessary. At this point, one of the options might well be a covert action. We know from long experience with covert action that it only makes sense as an adjunct to policy and should not be the policy itself.[24] Thus, the choice of using covert action remains with decision makers and is not chosen by intelligence. The conventional wisdom in some circles during the Cold War was that intelligence managers decided to mount covert actions independent of policy officials. (This notion that the CIA was a "rogue elephant" running amok was debunked during the famous investigations of intelligence held by Senator Frank Church in the 1970s. Church learned that all CIA covert actions had been directed in some way by the White House and funded in secret by members of Congress.[25])

Finally, decision makers at the top choose the option they desire and direct its implementation. In the case of covert action, this requires that the president issue a written finding that the covert action is needed. Then the appropriate intelligence official must brief the Intelligence Oversight Committees of Congress, in secret, about the policy "on a timely basis." Congress has often pressed presidents to issue the findings before the option is implemented, but presidents have usually chosen to ignore this, claiming that it infringes on their freedom of action.[26]

The pattern looks like this:

PROBLEM RECOGNITION
OPTION CREATION
OPTION SELECTION
IMPLEMENTATION

Intelligence analysis should feed into the process at all stages, but we know that the options that policy officials choose are driven by many things. Intelligence is not always at the top of the list.

CONSEQUENCES OF COVERT ACTION

Covert action has both short- and long-term consequences. This is true of all kinds of policy choices, but because covert action is kept secret, the normal debate about policy choices takes place among a relatively small group of people. The result is that short-term solutions, which may seem attractive at the time they

are chosen, may prove to have unintended consequences in the long run. There are too many examples to cover here, and the literature on covert action is voluminous. It is sufficient to say that U.S. governments rarely think about the long-term consequences of policy choices and, in that regard, covert action is no different from more open kinds of policies.

There is a long tradition in intelligence that intelligence officers do not offer policy recommendations to decision makers. Though this may be true for the delivery of finished intelligence products, it is not so in regard to covert action. As Dr. James Steiner, a former CIA officer, has pointed out, in covert action, especially in the war on terrorism, the attempt to be policy-neutral does not apply.[27] For many years, a senior CIA officer has been assigned to the White House staff to help work out the details of covert action when policy makers decide to have such operations.

This officer's role is to make sure that requested covert actions are feasible and supportable. Thus, the officer is as much a policy maker as an intelligence official.[28]

It is argued elsewhere in this chapter that one way to address the short-term versus the long-term consequences of covert action is to set up a center, much like the other interagency centers in U.S. intelligence. This center, however, should include both intelligence and policy officials. Its goal would be to analyze how a covert action might work and what its impact would be. The intelligence officers assigned to such a center should come from both the analytic and the operational units of the CIA. Traditionally, covert action has been kept compartmentalized within operations units, without the benefit of analytic inputs.

It seems pretty clear that presidents will always want to have the option of using some form of covert action against enemies and adversaries. No presidents in living memory, even those who were suspicious of covert action, have ever said that they would not use it. Therefore, the intelligence agencies that might be involved in such operations—primarily the CIA in the present U.S. intelligence community—must be prepared to be tasked to carry out covert action, and must maintain the capability to do so.

A FLAWED VISION

I suspect that, despite my preaching about alternatives to the traditional intelligence cycle, it will continue to be taught both inside government and elsewhere. Nonetheless, it would be encouraging to think that those so deeply wedded to the flawed concept of the intelligence cycle would, in the course of studying this volume, realize that there is an alternative to the traditional view of how intelligence works. Perhaps they might even consider it for discussion. Yet we know that people tend to look for confirming rather than disconfirming data. They will seek to defend the intelligence cycle, rather than consider the alternatives.

Nonetheless, the intelligence cycle is a flawed vision, and thus poor theory. One need only ask those who have toiled in the fields of intelligence.

NOTES

1. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press, 1966). I studied an earlier version published in 1948.

2. See, for example, Arthur S. Hulnick, "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach," *Intelligence and National Security* 1 (May 1986).

3. James Risen, *State of War: The Secret History of the CIA and the Bush Administration* (New York: Free Press, 2006).

4. The 9/11 Commission Report (New York: W.W. Norton, 2003), pp. 339–60.

5. Arthur S. Hulnick, *Fixing the Spy Machine: Preparing American Intelligence for the 21st Century* (Westport, CT: Praeger, 1999), p. 59.

6. Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31 (1978).

7. Arthur S. Hulnick, *Keeping Us Safe: Secret Intelligence and Homeland Security* (Westport, CT: Praeger, 2004), p. 16.

8. Risen, *State of War.*

9. Hulnick, *Keeping Us Safe*, pp. 85–86.

10. Roger Hilsman, *Strategic Intelligence and National Decision* (Glencoe, IL: Free Press, 1956).

11. "CSIS and the Security Intelligence Cycle," available at http://www.csis-scrs.gc.ca (accessed 1 April 2004).

12. Risen, *State of War*, pp. 39–60.

13. 9/11 Report.

14. Arthur S. Hulnick, "Indications and Warning for Homeland Security: Seeking a New Paradigm," *International Journal of Intelligence and CounterIntelligence* 18 (Winter 2005–6).

15. Hulnick, *Keeping Us Safe*, pp. 103–18.

16. See, for example, Pete Earley, *Confessions of a Spy: The Real Story of Aldrich Ames* (New York: G.P. Putnam's Sons, 1997).

17. Hulnick, *Keeping Us Safe*, p. 72.

18. Craig Whitlock and Walter Pincus, "Qaeda Deputy Mocks Bush," *Washington Post*, 31 January 2006.

19. Hulnick, *Keeping Us Safe*, pp. 126–27.

20. Hulnick, *Fixing the Spy Machine*, p. 81.

21. Ronald Kessler, *The Bureau: The Secret History of the FBI* (New York: St. Martin's Press, 2002).

22. Harold M. Greenberg, "The Doolittle Commission of 1954," *Intelligence and National Security* 20 (December 2005), pp. 687–94.

23. See, for example, Abram Shulsky and Gary Schmitt, *Silent Warfare* (Washington, DC: Brassey's, 2002).

24. James E. Steiner, "Restoring the Red Line Between Intelligence and Policy on Covert Action." *International Journal of Intelligence and CounterIntelligence* 19 (Spring, 2006), pp. 156–65.

25. See, for example, Rhodri Jeffreys-Jones, *The CIA and American Democracy*, 3rd ed. (New Haven, CT: Yale University Press, 2003).

26. Christopher Andrew, *For the President's Eyes Only* (New York: Harper Collins, 1995).

27. Steiner, op. cit.

28. Hulnick, *Fixing the Spy Machine*, pp. 82–83.

2

THE CHALLENGE OF GLOBAL INTELLIGENCE LISTENING

PATRICK RADDEN KEEFE

ON DECEMBER 20, 2005, THE *NEW YORK TIMES* revealed that under a new program initiated after the terrorist attacks of September 11, 2001, America's National Security Agency (NSA) had been conducting warrantless electronic surveillance inside the United States.[1] Though the Foreign Intelligence Surveillance Act (FISA), passed in 1978 in response to widespread abuses by the American intelligence community during the Vietnam years, had established a procedure whereby eavesdroppers must apply to a secret court for a warrant to monitor domestic communications, this new program circumvented that procedure altogether. In fact, the program relied on secret cooperation from major telecommunications companies, which built back doors into the hubs and switches through which phone calls and e-mails are routed, so that the NSA could gain unfiltered access to these communications flows.[2]

The ensuing scandal thrust the NSA into the national spotlight, occasioned a firestorm of public and congressional scrutiny of the very secretive business of signals intelligence, or SIGINT, and marked the first major debate about SIGINT activities since the congressional investigations that led to the passage of the FISA three decades earlier. As it happened, James Risen, the *Times* reporter who broke the story, had learned of the program a year earlier, but under pressure from the White House the newspaper had held off on publishing the piece.[3] That the *Times* should refrain from scrutinizing this most secret field of intelligence gathering was unsurprising; the American media has proved positively allergic to covering the NSA, despite the fact that it is the single largest intelligence agency in the country (and the world), with some 60,000 employees and an estimated budget of $6 billion.[4] Nor should it be surprising that the White House sought to quash the story. A studiously low profile has traditionally been

considered a sine qua non of any effective SIGINT operation—because if the enemy knows you are listening in, he will stop talking—and the National Security Agency has excelled throughout its history at making the general public forget that it even exists. ("No Such Agency," the old joke goes.) On those rare occasions when agency heads *have* emerged over the years to make statements in public, they have always intoned the same refrain: we gather foreign intelligence; we do not intercept the communications of Americans citizens. In this respect, the revelations in the *Times* amounted to nothing short of a reversal of everything that the intelligence community had been saying about the National Security Agency for the past thirty years. The episode also highlighted the three critical questions that must be addressed in any examination of this form of intelligence: Why is signals intelligence so secretive? How can SIGINT agencies effectively balance an aggressive pursuit of foreign adversaries with respect for legislative and constitutional constraints, and rigorous protection of personal privacy? And perhaps most important—and least often addressed—how effective *is* SIGINT as an intelligence tool?

SECRECY

During the Cold War, the United States and several of its closest allies developed an extraordinary global infrastructure for listening in. Allied cooperation on code-breaking during World War II was so effective that days after the Japanese surrender in 1945 President Harry Truman signed a top-secret, one-sentence memorandum, "to continue collaboration in the field of communication intelligence between the United States Army and Navy, and the British."[5] Out of that initial suggestion that cooperation on signals intelligence be carried on during peacetime grew a secret document, the UKUSA agreement, which formed the basis for another half century of intimate partnership between the United States, Britain, Canada, Australia, and New Zealand.[6] So longstanding and involved is the relationship established by UKUSA that today the National Security Agency operates and communicates much more closely with its sister eavesdropping agency, Government Communications Headquarters (GCHQ), in the United Kingdom, than it does with America's own CIA.

Throughout the Cold War, the NSA and its partners excelled at monitoring Soviet communications. The Soviets formed a relatively stable and predictable target: their political and military establishments were hierarchically arranged and organizational transition generally unfolded at a glacial pace, so UKUSA analysts had little trouble answering one of the crucial threshold questions in communications intelligence: Whom should we be listening to? Technologically, the actual eavesdropping was fairly easy: communications were bounced off of satellites and relayed between microwave towers. The air was so thick with electromagnetic signals that America's spies could erect aerials at "listening bases" around the planet and obtain a high-fidelity preview of enemy strategies

and maneuvers. It was like putting a cup out in the rain. Eventually dozens of these bases sprung up around the world, from Bad Aibling, in Germany, to Pine Gap in the desert of central Australia, to Menwith Hill, one of the largest eavesdropping stations on the planet, which continues to operate amidst the stone walls and pasturing cows of England's North Yorkshire moors. The NSA hired more mathematicians than any other organization on the planet, and its headquarters at Fort Meade, Maryland, housed one of the densest concentrations of computing power in history. Agency scientists prided themselves on being ten years ahead of consumer research and development.[7]

But the keystone on which this global eavesdropping empire was built was secrecy. As far back as the famous decision, by Admiral Sir William Hall, to delay acting on the Zimmermann telegram after British code breakers intercepted it, so as not to reveal Britain's interception capabilities, signals intelligence has been shrouded in secrecy.[8] The contemporary analog to the Zimmermann story involves a satellite phone used by Osama bin Laden during the 1990s, which the NSA was able to listen in on. After a Washington newspaper ran a story in 1998 suggesting that U.S. intelligence could intercept the phone, bin Laden stopped using the phone altogether. Michael Scheuer, who ran the CIA's bin Laden desk during that period, suggests that a direct causal line can be drawn between the publication of that story and the events of September 11.[9]

Cautionary tales of this sort have had a pronounced chilling effect in the willingness of the press—and of Congress—to rigorously examine the activities of America's eavesdropping agency. Though the *Times* was praised for breaking the wiretapping story, it had completely overlooked a major story several years earlier, in which it was revealed that the NSA and GCHQ had collaborated on an operation to monitor delegates to the United Nations Security Council in order to short-circuit any proposals for alternative resolutions that might send weapons inspectors back into Iraq. Despite the fact that the operation in question took place on the east side of Manhattan, the *Times* did not run a single news item on it.[10]

Timidity on the part of the press is in large part explained by the difficulty of securing any confirmation or comment on "sources and methods" from the studiously silent professional tribe of eavesdroppers. For employees at the NSA, an institutional fixation with secrecy represents the defining constraint of a career. After a year-long clearance process, new employees are exposed only to the need-to-know parameters of their own highly compartmentalized professional tasks. It is not unusual for someone working on a team in one room to have no idea whatsoever what precisely people down the hall are up to. An employee handbook describes "the security state of mind," and emphasizes that neighbors, family members, even spouses are not to be trusted with anything but the most generic account ("I work for the government") of what it is an individual does.[11]

At its most effective, the professional obsession with secrecy can transcend not only the ties of family and friendship, but the very instinct for survival. On April 1, 2000, a navy EP-3E reconnaissance plane, stuffed with sensitive

listening equipment and two dozen American eavesdroppers, collided with a jet over China. The EP-3E survived the crash intact but began to shake and abruptly dove toward the sea, plummeting 22,000 feet. After several minutes the pilot was able to regain some control and announced that they might be able to engineer a rough landing. As the pilot issued maydays and endeavored to steer the plane toward land, the eavesdroppers did not cry or pray or try to contact loved ones. They opened an air hatch and started madly shoving out stacks of classified documents, technical manuals, and frequency lists. While some crew jettisoned paper, others took an ax and began attacking the banks of sensitive equipment, denting and destroying it, doing anything to keep it from falling into Chinese hands. When the pilot managed to land the plane at Lingshui military airfield on Hainan Island, the dazed crew did not scramble out to the safety of land, but stayed in the plane, hand shredding documents as fast as they could. A Navy report later conceded, "The destruction of classified material was accomplished while the aircrew was probably still in shock from the aircraft collision and the subsequent rapid descent of the aircraft." Yet, remarkably, the report lamented the fact that not enough of the classified material onboard the EP-3E was adequately disposed of before Chinese officials boarded the plane, and called for better emergency destruction procedures in the future.[12]

The crew's disciplined one-track response to a crisis is emblematic of the culture of secrecy the NSA has managed to inculcate over its half-century existence, and it is indisputable that eavesdroppers must maintain a high degree of secrecy if they want to be successful. But there are important respects in which the culture of secrecy has been an impediment to the agency as well. A tendency to distrust not only potential foreign adversaries and the press, but also other elements in the American intelligence community, the academic world, and private-sector research and development organizations, has at times frustrated the NSA's working relationship within the intelligence bureaucracy and shut the agency off from promising recruits and new ideas. As the digital and Internet revolutions swept across the United States and around the world, the NSA had its head in the sand, divorced from the lightning-fast technological advances in Silicon Valley, complacent in its belief that agency scientists still had an edge on consumer research and development. By the time Lieutenant General Michael V. Hayden took over as director in March 1999, the agency looked increasingly like a dinosaur of the analog era.[13]

Hayden would go on to become Deputy Director of National Intelligence in 2005, and from the moment he arrived at NSA he adopted a radical new approach. Early in his tenure he announced "A Hundred Days of Change," aiming to undo the NSA's institutional arrogance and insularity, its attachment to outmoded technologies and procedures, and its refusal to take lessons from the outside world. Hayden talked to reporters and made speeches in public, in which he described the challenges the agency confronted. Some wondered whether this was not part of a considered strategy, in keeping with the fundamental tenets of communications interception, to lull adversaries into a false feeling of security.

But it was hard to argue with the basis of Hayden's assessment. In a 2000 lecture at American University, he pointed out that forty years ago, there were only 5,000 stand-alone computers, no fax machines, and no cell phones.

Today, there are over 180 million computers—most of them networked. There are roughly 14 million fax machines and 40 million cell phones, and those numbers continue to grow. The telecommunications industry is making a $1 trillion investment to encircle the world in millions of miles of high-bandwidth fiber-optic cable. They are aggressively investing in the future. As private enterprise has transitioned from the industrial age to the information age, so must government. So far, the National Security Agency is lagging behind.

Hayden acknowledged that a month earlier a software anomaly had caused the NSA to experience a seventy-two-hour network outage, during which it was unable to process or forward intelligence data, and even to communicate internally.[14]

Hayden envisioned a more open agency that was better able to adapt quickly to technological change. He also seemed to recognize that for an intelligence agency that always runs the risk, merely on the basis of its low profile, technical capabilities, and history of Vietnam-era abuses, of being typecast as an Orwellian menace, a small amount of openness can go a long way. James Bamford, the foremost civilian chronicler of the agency, met with suspicion and resistance while researching his ground-breaking book, *The Puzzle Palace*, in the late seventies and early eighties. But while preparing his follow-up volume, *Body of Secrets*, during Hayden's tenure, he found the agency much more accommodating. Hayden welcomed Bamford to the agency, granting him an extensive one-on-one interview, and arranging for a party on the occasion of the book's publication in 2001, to be thrown at NSA headquarters at Fort Meade.[15]

But the goodwill with which James Bamford thanked Hayden in his acknowledgments for "having the courage to open the agency's door a crack" was short-lived, as it would emerge in 2005 that despite his lip-service to openness and accountability, and the apparent hospitality with which he had welcomed Bamford, Hayden was in fact being less than straightforward. Hayden's decision to open the agency to scrutiny now appears to have been not a genuine commitment to a new culture of openness so much as a calculated and highly effective public relations gambit—an effort to neutralize the opposition. It was an irony, but by no means an accident, that the civilian who was granted the most unfettered access to the highest ranks of the National Security Agency was not in fact the one who broke the story about that agency's controversial warrantless eavesdropping program. And when the story was revealed, Bamford made no secret of his feelings of betrayal.[16] In fact, in a startling reversal, in January 2006, he joined a lawsuit against the Bush administration, alleging that the agency might have eavesdropped on him, and remarking that the secret program represented "a return to the bad old days of the NSA."[17]

In fact there had been signs even before the wiretapping revelations that in the context of the war on terror, the eavesdropping agency was retreating

from view once again. Despite its central role in the intelligence community, the agency merited only the briefest of mentions in the final report of the 9/11 Commission.[18] Throughout the debates in the years following the terrorist attacks about the function, dysfunction, and structure of the U.S. intelligence community, and NSA was an elephant in the room—a factor of enormous importance that politicians and pundits studiously avoided. In fact, no outcry or discussion greeted the news in December 2003 that the agency had won the authority to automatically turn down requests by U.S. citizens, pursuant to the Freedom of Information Act, for records on the NSA. The agency argued that this was a "labor saver," because officials were wasting too much time processing various requests for information about NSA's operations, only to reject them all anyway.[19]

PRIVACY

More than other types of spying, SIGINT is unsettling to the general populace and its elected representatives, and gives rise to a range of concerns about the protection of privacy and civil liberties. The veil of secrecy that shrouds this kind of activity from public scrutiny or legislative oversight and the demonstrably intrusive technologies that are now available to the enterprising snoop mean that an agency like the NSA will always have a major challenge when it comes to winning the public's trust. When Henry Lewis Stimson was appointed Secretary of State by President Herbert Hoover in 1929 and learned that American code breakers had been intercepting and reading the communications of British, French, Italian, and Japanese diplomats, he famously declared, "Gentlemen do not read each other's mail." But on the contrary, the history of American SIGINT has involved a tendency not only to monitor diplomats and generals, but the public at large as well.

After the abuses of the 1960s and 1970s, in which the NSA cooperated with private companies to monitor international cables entering and leaving the United States, and intercepted the communications of such civilian antiwar protesters as Jane Fonda and Dr. Benjamin Spock, the Foreign Intelligence Surveillance Act was designed to create a wall between foreign intelligence and domestic law enforcement operations. But having passed this landmark piece of legislation, Congress left the law to do the work on its own, and, discouraged by the NSA's penchant for secrecy and the technical complexity of the activities in question, effectively abdicated its role as an oversight mechanism.

In principle the House and Senate Intelligence Committees are authorized to ensure that the National Security Agency operates effectively and within the letter of the law, but in practice, the members of these committees are not cleared to hear the most secret details of the NSA's most significant operations and they enjoy few prerogatives in determining budgets that the more powerful Armed Services and Appropriations Committees cannot undo. Norman Minetta, who

served on the House Intelligence Committee during the Reagan years, famously remarked of the relationship between the committee and the intelligence community, "We are like mushrooms. They keep us in the dark and feed us a lot of manure."[20] More recently, Bob Kerrey, who was the ranking Democrat on the Senate committee in the 1990s, said that many senators only serve on the committee for the travel opportunities.[21]

Though the warrantless eavesdropping program generated a great deal of press and debate, it was hardly the first instance since the 1970s in which the NSA had revealed an institutional tendency to overreach in its duties, play fast-and-loose with legal constraints, and potentially infringe upon the privacy of innocent American citizens. Two years before September 11, then Chair of the House Intelligence Committee Porter Goss asked the NSA's general counsel for the internal legal guidelines that govern when the agency could and could not eavesdrop on the conversations of U.S. citizens. The rationale for Goss's request was straightforward:

> If the NSA General Counsel provided too narrow an interpretation of the agency's authorities, it could hamper the collection of significant national security and intelligence information. If, on the other hand, in its effort to provide timely intelligence to the nation's policy makers, the NSA General Counsel construed the Agency's authorities too permissively, then the privacy interests of the citizens of the United States could be at risk.

The matter was clearly one of line-drawing—precisely the kind of line-drawing between robust intelligence and civil liberties that the committees were created to oversee. The agency stonewalled, however, citing a Procrustean extension of attorney-client privilege, whereby any document that happened to be sitting on the desk of an NSA lawyer did not have to be handed over to Congress.[22]

Shortly after September 11, it became clear that the FISA system, which was widely acknowledged to be a rubber stamp, was nevertheless inviting abuse on the part of those seeking surveillance warrants. In May 2002 the famously circumspect secret court established by the FISA to review applications for wiretapping warrants, took the unprecedented step of publishing a 7-0 decision. The court, which approved about 10,000 warrant applications between the passage of FISA and September 11, rebuked the Justice Department and the FBI for providing wrong information in 75 post-9/11 applications for search warrants and wiretaps. The FISA judges called for stricter policing of FISA's delineation between domestic law enforcement and foreign intelligence operations to "protect the privacy of Americans in these highly intrusive surveillance searches."[23]

More dramatic, but largely overlooked, was the disclosure in the spring of 2005, during the Senate confirmation hearings on John Bolton's candidacy for the position of U.S. Ambassador to the United Nations, that the NSA was giving policy makers and other intelligence agencies information about U.S. citizens. Even as enshrined in the FISA, the prohibition on domestic spying without a

warrant has always been something of a legal fiction: the standard practice is to go ahead and eavesdrop on the conversations of foreigners, even if the party on the other end of the line is an American citizen. Summaries of these conversations are then routinely distributed throughout the relevant government agencies. The privacy of the American citizens involved is putatively preserved by replacing their names with the phrase "U.S. person" in the summary. During the Bolton hearings, however, it emerged that when he was at the State Department, Bolton on several occasions received summaries of intercepts between foreigners and "U.S. persons" and requested that the spy agency tell him who those Americans were. Without asking Bolton to show any cause for his request or going through a review process, the agency complied. Following this revelation, *Newsweek* discovered that from January 2004 to May 2005 the National Security Agency had supplied names of some 10,000 American citizens in this informal fashion to policy makers at many departments, other American intelligence services, and law enforcement agencies.[24] Bolton told Congress that he asked the spy agency for the names in order "to better understand" summaries of intercepted conversations: "It's important to find out who is saying what to whom." Stewart Baker, a former General Counsel at the NSA, has essentially conceded that the requests were vetted with a rubber stamp. "We typically would ask why" disclosure of an identity was necessary, he said, "but we wouldn't try to second-guess" the rationale.[25]

But whereas the Bolton revelations did not strike a powerful cord with the American public or the press, the revelations some six months later that the NSA was engaged in a warrantless surveillance program of American citizens did. In some respects, it would have been naive to believe that the wall erected by the FISA between foreign intelligence and domestic law enforcement had any hope of enduring in a conflict with terrorist cells that are able to strike from within the United States. And in the wake of the initial revelations it emerged that during the years since September 11, the NSA had been in the process of quietly turning its electronic ear, which had traditionally been oriented outside America's borders, inward.

According to reports on the program, the NSA adopted a wholesale approach, tapping directly into commercial communications arteries, and implicating thousands of innocent civilians in the process. Officials familiar with the program describe a broad-based operation, involving data mining, link analysis, and pattern recognition technologies, which seeks not to listen in to everybody all the time, but rather to scan communications traffic and correlate that data with records from public and private databases to answer a more difficult question: Whom should we be listening to? "Metadata" is the technical name for the routing information associated with a communication—the initiator, recipient, time, and duration of a phone call, or the header information on an e-mail. The NSA program scanned the metadata of thousands, and possibly millions, of communications, performing a kind of social network analysis. When asked about the program, President George W. Bush replied, "If Al Qaeda is calling you, we want

to know why." But it seems that in addition, we want to know who you are calling, and who those people are calling. Russ Tice, a former NSA employee who worked on highly classified Special Access Programs, says that NSA analysts start with a suspect and "spiderweb" outward, looking at everyone he contacts, and everyone those people contact, until the list includes thousands of names.[26]

Leaving aside for a moment the dubious legality of this technique, it does seem that such a mile-wide-and-inch-deep review of communications might in fact be less unsettling to the average American than some more comprehensive form of surveillance. Having a computer monitor the metadata of one's communications will reveal less private truths than having a human analyst actually listening to or reading one's words. If in fact you are not calling Al Qaeda, you might assume, you should be of no interest to intelligence analysts, and you will be discarded by the computers that sort the wheat from the chaff on the first level of review.

The problem with this reassuring scenario is that it fails to take into account the danger of false positives. Most people are connected by two degrees of separation to thousands of people, and by three degrees to hundreds of thousands. Thus, even a terrorist hiding out in some mid-sized American city, with a bare minimum of social interactions and acquaintances, could be linked, however tangentially or coincidentally, to innocent civilians. In fact, reports indicate that the overwhelming majority of the leads generated by the NSA program have been false positives—innocent civilians implicated in an ever-expanding associational web. When the Federal Bureau of Investigation (FBI) received a fresh batch of tips from the NSA program, agents joked that this meant "more calls to Pizza Hut."[27] The National Counterterrorism Center's database of suspected terrorists contains 325,000 names—a number which, logic would suggest, must include at least tens of thousands of innocent false positives; the Congressional Research Service recently found that the NSA is at risk of being "drowned" in information.[28]

EFFICACY

The British intelligence writer James Rusbridger once remarked, "It is frequently said about advertising that half the money spent is wasted but no one knows which half. Much the same could be said about intelligence." The particular matter of false positives raises a vexing and enduring question: Just how effective is signals intelligence?[29]

One oft-repeated lesson of September 11 was that the United States had relied too heavily during the 1990s on intelligence gathered by remote control—listening bases, satellites, and other gadgets that seemed to take the place of old-fashioned human intelligence assets. In the post–Cold War period, the United States had fewer than 5,000 spies, all told, and over 30,000 eavesdroppers.[30] The

colossal intelligence failure that led to the events of September 11 might have presented an opportunity to re-examine that ratio, and perhaps recalibrate priorities and allocations within the intelligence community. Yet as of May 2004, thirty-two months after the attacks, the CIA's Directorate of Operations had about 1,100 case officers posted overseas—fewer than the number of FBI agents assigned to the New York City field office alone.[31] The intelligence community was investing enormous amounts of money in various artificial intelligence computer programs that effectively wrote the human analyst out of the equation, by scanning massive volumes of information for telltale patterns or identities and sounding an alarm when something looked amiss. At precisely the juncture when effective human spies, with a strong grasp of local cultures and languages, should have been coming to the fore once again, the intelligence community seemed more bent than ever on devising technological crystal balls that would produce timely, actionable information at the touch of a button.[32]

It went largely unremarked that the single biggest item in the U.S. intelligence budget for 2005 was an enormously expensive "stealth" reconnaissance satellite, built by Lockheed Martin for the National Reconnaissance Office, and code-named Misty. Despite the fact that the Senate Intelligence Committee vetoed Misty two years in a row, and that one senator who was briefed on its details described it as "unnecessary, ineffective, over-budget, and too expensive," and revealed that several independent reviews found that other programs already in existence or development could produce the same intelligence at far less cost and technological risk, Misty was saved by the Appropriations Committee. Photo reconnaissance satellites were ideal tools for monitoring Cold War targets, but their utility in current conflicts is questionable. Monitoring nuclear powers with eyes in the sky is a gamble, because many foreign adversaries know when America's satellites are overhead, and can time their operations accordingly.[33] There is evidence that terrorists have caught on as well—American forces in Afghanistan recovered Al Qaeda manuals describing the orbits of U.S. satellites.[34] And in any event, overhead assets are better suited to monitoring Soviet tank divisions than a convoy in the desert or an arms deal in a village square. Moreover, Misty's price tag—$9.5 billion, amortized over several years—will inevitably put a dent in the intelligence community's ability to invest in other types of training and assets. Budget allocations are fundamentally a zero-sum game, and a windfall for one agency or program means cutbacks for another. A single human analyst or operative costs the government less than $200,000 a year, including salary, benefits, and the computer on the desk. In the words of one official who objected to Misty, "With the amount of money we're talking about here, you could build a whole new CIA."[35]

The Misty controversy—or rather, the lack thereof—is an object lesson in the misguided and mutually contradictory priorities of the intelligence community in the years since 2001, and an indication of the strange refusal to hold various intelligence programs to a results-based bottom line. In a Spring 2002 article called "Time for a Rethink," the *Economist* posed a pithy hypothetical:

> Imagine a huge $30-billion conglomerate. It operates in one of the few businesses that might genuinely be described as cut-throat. Its competitors have changed dramatically, and so have its products and technologies. But its structure is the same as when it was founded, in 1947. Nobody leads this colossus (there is just an honorary chairman) and everyone exploits it. Demoralized and bureaucratic, it has just endured its biggest-ever loss. The response: the firm has been given even more money, and nobody has been sacked.[36]

The scenario captures the peculiar paradox of the intelligence agency. The nature of the job is such that some measure of failure is more or less inevitable. But the human stakes involved are so high that failure cannot properly be penalized. On the contrary, given that it is the appearance of weakness that can really move money in Washington, it is often the case that failure is rewarded. The intelligence historian Rhodri Jeffreys-Jones regards this as a cycle, wherein appropriations-hungry intelligence agencies "con" Congress into throwing more funding their way in times of crisis. "A disaster happens," Jeffreys-Jones writes. "The government sets up a preemptive inquiry to deliberate until the fuss dies down; the confidence men now say the disaster happened because they had too little money to spend on intelligence; the President and Congress authorize more intelligence funds." He points out that the CIA and the NSA were born out of the intelligence failure at Pearl Harbor, and that the NSA's technical shortcomings in the 1990s inspired not punitive cuts, but larger appropriations.[37]

Jeffreys-Jones may overstate the case somewhat, and it may be absurd to adopt the corporate model that underlies the *Economist*'s hypothetical, which would hold that you could penalize an organization for failing. The intelligence community is not a corporation, after all. Any penalties levied against it could be felt by the entire country, if it meant that agencies were less vigilant for any period of time. But especially in areas where expensive new technologies play a role, it does seem that there is a tendency to throw good money after bad: the NSA, with its colossal global eavesdropping infrastructure, failed to hear so much as a whisper in advance of the September 11 attacks. But rather than judge this type of intelligence harshly, the tendency is instead to reinvest, assuming that it could only have been a funding shortage that was to blame for the intelligence failure, and not some flaw in the very model of that intelligence capability itself.

Raw interception power is not the primary problem for signals intelligence agencies. The NSA intercepts some 650 million communications worldwide every day.[38] Every three hours its satellites collect enough information to fill the Library of Congress.[39] Russ Tice, the former NSA employee, says that the domestic wiretapping program could end up netting a number of potential suspects that is "in the millions."[40] The real challenge is making sense of all of that information in a timely manner. In fact, where SIGINT is concerned, a paradox seems to be built into the traditional "intelligence cycle," in which the collection of raw intelligence and the production of actionable intelligence are part of a mutually reinforcing process. In SIGINT, the better one becomes at collection, the more

difficult it is to do good production. On September 10, 2001, the NSA intercepted two phone calls between Al Qaeda affiliates in Saudi Arabia and Afghanistan. One said, "The match begins tomorrow," and the other, "Tomorrow is the Zero Hour." But no one translated these two intercepts until September 13.[41] This sort of story suggests that the NSA's ability to gather haystacks is far outpacing its ability to locate needles.

Even assuming that the threshold question about whom precisely SIGINT analysts should be tracking is answered—and that is a significant assumption, in light of the number of false positives reportedly generated by the "terrorist surveillance program"—there is still the matter of translating those intercepted communications. Even as the cryptologists at the NSA devise new means of breaking strong encryption algorithms, a foreign language can prove as strong a defense for adversaries as an actual code. As a result of a shortage of linguists—not just in Arabic, but in Farsi, Pashto, and other languages spoken in countries where Al Qaeda recruits—a considerable backlog of intercepted but untranslated calls has developed. As of the summer of 2005, the FBI's cache of untranslated counterterrorism wiretaps was an astonishing 8,000 hours long.[42]

While there has been some effort to train more linguists, the shortage remains severe. In 2002 American colleges granted a mere six undergraduate degrees in Arabic.[43] Moreover, Arabic of the sort taught in American colleges is rather like Shakespearean English, and would not provide much help in listening to the conversations of people who speak contemporary, regional dialects. The best way to prepare to really comprehend these spoken conversations is to spend time in the countries in question, immersing oneself in the local language and culture. But as it happens, a summer vacation spent in Egypt or Syria represents a serious security liability in the NSA recruitment and clearance process.[44] Thus, ironically, the kind of experience that is a precondition to actual fluency in a target language is also grounds for disqualification by our nation's intelligence agencies.

Reverting again to a preference for the technical over the human, the intelligence community has sought to get around this problem by investing in a variety of new technologies that might supplant the human translator, and interpret written and spoken foreign language conversations in real time.[45] But although automated translation may represent a research and development holy grail for intelligence agencies, an actual realization of that objective, with accuracy rates that approach reliable, remains a long way off, and many linguists argue that a computer will never grasp nuances of tone—such as sarcasm, exaggeration, or humor, much less idiom, metaphor, or allusion—that a well-trained human analyst can.

And this points to an even graver challenge for signals intelligence. Assume for a moment that in addition to resolving the threshold question of whom one should be targeting, we could conjure some magic algorithm that would resolve the translation problem as well. We would be left with a real-time stream of literally translated communications between suspected adversaries. But what

good would that do? Assume that the two September 10 phone calls had been translated on September 10, and distributed through various intelligence and defense channels in a timely manner. What kind of actionable intelligence would, "Tomorrow is the Zero Hour," and "The match begins tomorrow" provide? Mike Hayden told Congress that during the three months prior to 9/11 the agency intercepted thirty such messages obliquely promising imminent disaster.[46] In fact, some intelligence officials have suggested that those two calls referred not to the terrorist attacks in New York and Washington at all, but to the assassination of Sheikh Masood, the Northern Alliance leader in Afghanistan, which took place the day before the call.[47]

Even promptly intercepted, interpreted, and reported, language is at best an opaque eyeglass through which to deduce the plans and activities of an adversary. Perhaps the most telling instance of the intelligence community's overestimation of the reliability of language was Secretary of State Colin Powell's presentation before the United Nations Security Council on February 5, 2003, in which he laid out America's case for war with Iraq. During the presentation Powell played three communications intercepts. He sought to demonstrate, among other things, that Saddam Hussein's Iraq was producing nerve agents, and played a conversation that had been intercepted just weeks before, between two commanders in Iraq's Second Republican Guard Corps. In the intercept, one commander tells the other to remove the expression "nerve agents" wherever it comes up in a particular communication. In the months preceding Powell's presentation, Mike Hayden had personally ordered that $300 million to $400 million of the NSA's annual budget be redirected to "Iraq unique" operations and targets, and this was the fruit of those efforts.[48] Powell asserted that the conversation confirmed the administration's "conservative estimate" that Iraq had a stockpile of between one and five hundred tons of chemical-weapons agents. "That is enough agent to fill sixteen thousand battlefield rockets," he said. "Even the low end of one hundred tons of agent would enable Saddam Hussein to cause mass casualties across more than one hundred square miles of territory, an area nearly five times the size of Manhattan."[49]

Yet eight months after Powell's presentation David Kay, the weapons inspector appointed by the administration to run the CIA's Iraq Survey Group, told the congressional intelligence committees that he could produce no evidence of nerve agents. In fact, he went so far as to say that to the best of the group's knowledge, there had been no chemical-weapons program in Iraq since 1991.[50] So what, one wonders, were those two Iraqi officials talking about? We may never know the answer, but the episode should at the very least insert a note of serious caution into any discussion of the promise of eavesdropping as an intelligence tool: even without the very real challenges of identifying targets, surreptitiously collecting their communications, and translating and analyzing those communications in a timely manner, SIGINT will offer no panacea to intelligence officials. In the final analysis, any conversation to which you are not

a party will be something of a Rorschach blot: The parties might very well be saying what you think they're saying. But then again, they might not be.

CONCLUSION

Whatever its actual, operational shortcomings, signals intelligence offers, in theory, a kind of strategic omniscience, and as such it is unlikely that there will be any diminution in the resources accorded to it, or the freedom from oversight or bottom-line scrutiny it enjoys. After promising an aggressive investigation after the December 2005 revelations about warrantless eavesdropping, Congress essentially conceded defeat, calling no NSA officials to testify, and failing to take any creative measures, such as subpoenaing the CEO's of the cooperating telecommunications companies, in order to establish even the broadest parameters of the program. Though some had predicted another investigation of intelligence abuses like the congressional hearings of the 1970s, it was soon clear that this was not to be.

The relationship between secrecy, privacy, and efficacy in signals intelligence could not have been more clearly on display: the official secrecy surrounding the NSA's activities was so forbidding that Congress could not assure the American people that the program incorporated satisfactory safeguards for civil liberties and individual privacy, much less that so bold a departure from the established FISA system was at least justifiable on the grounds of its effectiveness in detecting and capturing terrorists. Lost in the Judiciary and Intelligence Committee's meek proceedings was the warning, from President Bush's own "secrecy czar," J. William Leonard, that "secrecy comes at a price—sometimes a deadly price."[51]

Behind the veil of classified Washington it is likely that America's SIGINT apparatus will continue to grow. Jihadist terrorist groups may take the form of decentralized, difficult-to-detect networks, but these networks rely for their survival, and for their operations, on the kinds of connective links that can only be provided by modern communications technologies. Telephone calls, e-mails, and wire transfers are what connect a sleeper cell in one country with logistical masterminds in another, and so it is only natural that U.S. intelligence will endeavor to pursue terrorist adversaries by searching for and, when possible, monitoring these connections.

As the white noise of contemporary networked communications broadens and intensifies, however, it will be a major challenge for America's SIGINT analysts to quickly ferret out communications that are of interest. It seems likely that any effort to address this problem with a purely, or predominantly, technological approach will both undermine individual privacy and prove so plagued by false positives that the results will be dangerously inefficient. But unless some accommodation is made between the NSA and Congress such that rigorous, closed-door scrutiny of the agency's work is possible, a significant danger remains that

the formidable resources of America's eavesdropping apparatus will fail to safeguard privacy, while at the same time failing to keep the country safe.

NOTES

1. James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 20, 2005.

2. See James Risen, *State of War: The Secret History of the CIA and the Bush Administration* (New York: Free Press, 2006), pp. 42–60; Scott Shane, "Attention in NSA Debate Turns to Telecom Industry," *New York Times*, February 11, 2006.

3. Gabriel Sherman, "Why Times Ran Wiretapping Story, Defying Bush," *New York Observer*, December 26, 2005.

4. On the number of employees, see James Bamford, *Body of Secrets* (New York: Doubleday, 2001), p. 482. On the annual budget, Bob Woodward, *Plan of Attack* (New York: Simon and Schuster, 2004), p. 213.

5. Bradley F. Smith, *The Ultra-Magic Deals and the Most Secret Special Relationship, 1940–1946* (Navato, CA: Presidio, 1982), p. 212.

6. On the UKUSA arrangement generally, see Jeffrey Richelson and Desmond Ball, *The Ties That Bind*, 2nd ed. (Boston: Unwin & Hyman, 1990).

7. For the definitive history of the agency in these years, see James Bamford, *The Puzzle Palace* (New York: Penguin, 1983).

8. Barbara Tuchmann, *The Zimmermann Telegram* (New York: MacMillan, 1996).

9. The original article containing the information was by Ernest Blazar, "Inside the Ring," *Washington Times,* August 24, 1998. Scheuer made the remarks at the first annual National Intelligence Conference, in Arlington, Virginia, on February 8, 2005. When administration officials cited this story in critiquing the *New York Times* for revealing the domestic wiretapping operation, some press accounts questioned whether in fact that *Washington Times* story was what actually prompted bin Laden to stop using the phone, and argued, in effect, that the story of bin Laden's satellite phone has become a kind of old wives' tale. See Glenn Kessler, "File the bin Laden Phone Leak Under 'Urban Myths,' " *Washington Post*, December 22, 2005.

10. See Patrick Radden Keefe, "The Leak Was Me," *New York Review of Books*, June 10, 2004.

11. See "NSA Security Guidelines Handbook," available at http://www.tscm.com/NSAsecmanual1.html (accessed March 1, 2005).

12. "China 'Likely' Saw U.S. Secrets," Associated Press, September 12, 2003; Bill Gertz, "China Blamed in '01 Air Collision," *Washington Times*, September 13, 2003; "Beijing Gets Voice Data From Plane," *Washington Times*, May 15, 2001.

13. See Seymour Hersh, "The Intelligence Gap," *New Yorker*, 1999.

14. Lieutenant General Michael V. Hayden, USAF, Director, National Security Agency, Address to Kennedy Political Union of American University, February 17, 2000.

15. See James Bamford, *Body of Secrets* (New York: Doubleday, 2001), and "Director of NSA Shifts to New Path," *Baltimore Sun*, August 8, 2004.

16. Scott Shane, "Leader Who Worked to Reshape Agency's Image Is on the Defensive," *New York Times*, January 24, 2006.

17. Eric Lichtblau, "Two Groups Plan Lawsuits Over Federal Eavesdropping," *New York Times*, January 17, 2006.

18. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: Norton, 2004).

19. "NSA Can Summarily Reject Requests for Information," *Baltimore Sun*, December 11, 2003.

20. Loch K. Johnson, *A Season of Inquiry: Congress and Intelligence* (Chicago: Dorsey Press, 1998), p. 263.

21. Author's interview with Senator Bob Kerrey, New School for Social Research, New York, February 3, 2004.

22. Additional views of Chairman Porter Goss, Intelligence Authorization Act for Fiscal Year 2000, 106th Congress, 1st Session, Part 1, Report 106-30, May 7, 1999.

23. *In All Matters Submitted to the Foreign Intelligence Surveillance Court*, United States Foreign Intelligence Surveillance Court, May 17, 2002, available at http://www.fas.org/irp/agency/doj/fisa/fisc051702.html (accessed March 1, 2006).

24. Mark Hosenball, "Spying: Giving Out U.S. Names," *Newsweek*, May 2, 2005.

25. Patrick Radden Keefe, "Big Brother and the Bureaucrats," *New York Times*, Op-Ed Page, August 10, 2005.

26. Brian Ross, "NSA Whistleblower Alleges Illegal Spying," ABC News, January 10, 2006.

27. Barton Gellman, Dafna Linzer, and Carol D. Leonnig, "Surveillance Net Yields Few Suspects," *Washington Post*, February 5, 2005; Lowell Bergman, Eric Lichtblau, Scott Shane, and Don Van Natta Jr., "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," *New York Times*, January 17, 2006. See also Patrick Radden Keefe, "The Kevin Bacon Defense," *New York Times Magazine*, March 12, 2006.

28. Walter Pincus and Dan Eggen, "325,000 Names on Terror List," *Washington Post*, February 15, 2006; "Data Mining and Homeland Security: An Overview," Congressional Research Service Report, January 27, 2006.

29. James Rusbridger, *The Intelligence Game* (New York: New Amsterdam, 1989), p. 1.

30. "Time for a Rethink," *Economist*, April 18, 2002.

31. Douglas Jehl, "Abundance of Caution and Years of Budget Cuts Are Seen to Limit CIA," *New York Times*, May 11, 2004.

32. See "Data Mining and Homeland Security: An Overview," Congressional Research Service Report, January 27, 2006.

33. Patrick Radden Keefe, "I Spy," *WIRED*, February 2006.

34. Eli Lake, "Noise Pollution," *New Republic*, November 4, 2002.

35. Dana Priest, "New Spy Satellite Debated on Hill," *Washington Post*, December 11, 2004.

36. "Time for a Rethink," *Economist*, April 18, 2002.

37. Rhodri Jeffreys-Jones, *Cloak and Dollar* (New Haven, CT: Yale University Press, 2002), p. 9.

38. Michael Hirsh, "Wanted: Competern Big Brothers," Newsweek.com, February 8, 2006.

39. Michael Erard, "Translation in the Age of Terror," *Technology Review*, March 2004.

40. Brian Ross, "NSA Whistleblower Alleges Illegal Spying," ABC News, January 10, 2006.

41. "Al-Qaeda Tied to Intercepted Phone Calls," CNN.com, June 20, 2002; Scott Shane, "Coded Warnings Become Clear Only in Light of Sept. 11 Attacks," *Baltimore Sun*, June 21, 2002.

42. Dan Eggen, "FBI Faulted on Unreviewed Wiretap Recordings," *Washington Post*, July 28, 2005.

43. Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, *Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002.

44. Patrick Radden Keefe, "Spy World," *Boston Globe*, February 13, 2005.

45. See Chip Walter, "The Translation Challenge," *Technology Review*, June 2003.

46. Statement for the Record by Lieutenant General Michael V. Hayden, USAF, Director, National Security Agency/Chief, Central Security Service, Before the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, October 17, 2002.

47. "Terror Intercepts on Eve of Sept. 11 Too Vague—NSA," Reuters, October 17, 2002.

48. Bob Woodward, *Plan of Attack* (New York: Simon and Schuster, 2004), p. 217.

49. Colin Powell, Remarks to the United Nations Security Council, February 5, 2003.

50. See Thomas Powers, "The Vanishing Case for War," *New York Review of Books*, December 4, 2003.

51. Formal Statement, J. William Leonard, Director, Information Security Oversight Office, National Archives and Records Administration, Before the Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations. U.S. House of Representatives, March 2, 2005.

3

PROMETHEUS EMBATTLED

A Post–9/11 Report Card on the National Security Agency

MATTHEW M. AID

THERE IS NO QUESTION THAT THE NATIONAL SECURITY AGENCY (NSA) is today one of the most important components of the U.S. intelligence community, if not the most important and powerful intelligence agency in the United States. Before September 11, 2001, the 32,000-strong NSA was struggling to reform and modernize itself with mixed success. Today, the Agency's manpower is rapidly climbing toward 40,000 people, and its budget has topped the $4 billion mark. Its power, however, is not derived from its massive size and budget. Rather, it stems from the fact that the Agency produces the majority of the actionable intelligence coming out of the U.S. intelligence community today. Prior to the 9/11 disaster, approximately 60 percent of the intelligence information contained in the Top Secret Codeword *President's Daily Brief* (PDB) sent to the president of the United States every morning was based on signals intelligence (SIGINT) coming out of the NSA. Today, this number is even higher as the NSA's access to global telecommunications has expanded dramatically in the five years since the 9/11 tragedy.[1] The NSA's standing with the White House and the Pentagon has been helped by the fact that the Central Intelligence Agency (CIA), formerly the NSA's chief competitor within the U.S. intelligence community, has been in a state of freefall since 9/11, with senior intelligence officials describing the current state of the Agency as being one of "chaos and disintegration."[2]

The slow but steady rise of the NSA to the top of the U.S. intelligence community can be traced back to the end of World War II in 1945, and the subsequent shift within the U.S. intelligence community to monitoring America's new principal global protagonist, the Soviet Union. Most of the NSA's accomplishments during the forty-year-long Cold War, of which there were many, remain classified, but two decades of research by the author indicates that during the Cold War, the NSA and

its foreign SIGINT partners provided more reliable intelligence on the Soviet Union and its allies than the rest of the U.S. intelligence community combined, with perhaps the exception of the spy satellites of the National Reconnaissance Office.[3]

And yet, despite its many accomplishments during the Cold War, it is now clear that the NSA, like the rest of the U.S. intelligence community, lost its way in the decade after the fall of the Berlin Wall and the collapse of the U.S.S.R. in 1991. The ten-year period from 1991 to 2001 inside the NSA was marked by declining fiscal and manpower resources, poor internal management, and a pervasive bureaucratic inertia that effectively stifled demands for change both from within and outside the Agency. Between 1991 and 1996, the NSA lost one-third of its staff, and its budget was slashed by 35 percent from $5.2 billion to less than $3.5 billion.[4] We now know that these cuts, especially the loss of so many of the Agency's most talented managers, had a devastating impact on the NSA's ability to perform its mission. According to a declassified congressional study: "One of the side effects of NSA's downsizing, outsourcing and transformation has been the loss of critical program management expertise, systems engineering, and requirements definition skills."[5] The NSA's Inspector General, Joel F. Brenner, has written that the 1990s for the NSA was "a decade of under-funding and, in the view of some critics, indifferent management" that left the Agency "behind the curve" in terms of staying abreast of the dramatic changes then taking place in the global telecommunications infrastructure."[6] By the end of the 1990s, the Agency found itself swamped by millions of intercepted radio messages, telephone calls, and e-mail messages, as well as millions of terabytes of digital data traffic, such as bank money transfer messages, which NSA overworked analysts just could not keep up with, much less digest.[7] The NSA also failed to adequately address itself to the rapid proliferation of new intelligence targets that it was required to confront in the post–Cold War era, such as international terrorism, narcotics trafficking, global economics and trade issues, and the proliferation of weapons of mass destruction (WMD) technology around the world. This was coupled with the inability on the part of senior Agency officials to come to grips with the dramatically changing nature of the global telecommunications infrastructure. The NSA's intelligence production declined precipitously during the 1990s, and the Agency's customers inside the U.S. government became increasingly unhappy with both the quantity and quality of the NSA's intelligence output. All in all, the NSA was in trouble and desperately needed someone to shake things up and bring much-needed change to an Agency that historically had resisted attempts at reform.[8]

GENERAL HAYDEN'S MODERNIZATION AND REFORMATION EFFORT

On February 23, 1999, the Pentagon announced that the new Director of the NSA was to be U.S. Air Force Major General Michael V. Hayden, who was finishing a tour of duty in Seoul, South Korea, as the Deputy Chief of Staff of the

United Nations Command and U.S. Forces in Korea. General Hayden, age 52, was a veteran intelligence officer who had previously held a number of high-level intelligence and policy positions, including commanding the Air Intelligence Agency from January 1996 to September 1997. He had also previously served as the Director of Defense Policy and Arms Control in the National Security Council (NSC) from September 1989 to July 1991.[9]

As noted above, General Hayden inherited a deeply troubled organization. James R. Taylor, the Deputy Director for Operations, told Hayden a month after he took office: "We have good people [working] in a flawed system."[10] After considering all of his options, in October 2000 General Hayden publicly unveiled an ambitious plan to completely reform and modernize the Agency.[11]

The price tag for General Hayden's modernization programs was staggering, even by Washington standards. In 2000, NSA planners put a price tag of a whopping $12 billion on the full range of modernization options then being proposed. A review of the program reduced the price tag to $8 billion by the end of 2001, but everyone at the NSA knew that there was no way that Congress would approve this figure, even in the post-9/11 era. By mid-2002 the NSA had reduced the modernization price tag down to approximately $5 billion, with the costs of the program spread out over a ten-year period.[12]

General Hayden moved quickly to implement the outlines of his modernization program. Dramatic changes took place at the NSA before the October 2000 reform plan had to be altered because of the tragic terrorist attacks on New York and Washington on September 11, 2001. General Hayden completely restructured the NSA's senior management staff, fired or transferred a number of senior managers who opposed his reform plans, and cut the number of management committees involved in high-level policy making down to just one. General Hayden brought in a number of senior managers from the business world to help him reshape the Agency's management practices.

In February 2001 there was a dramatic reorganization of the internal operating structure of the NSA, which put "front-end" operations in the hands of just two organizations: the Signals Intelligence Directorate and the Information Assurance Directorate. All other nonoperational supporting functions were transferred to the director's office.[13] Hayden also immediately ordered a reduction in the size of the NSA's bloated workforce. In November 1999, the NSA cut its civilian personnel by 7.5 percent from 18,945 to 16,753 people, and the following year reduced the size of the Agency's military staff by 10 percent. The NSA also deactivated a number of older SIGINT collection sites, consolidated the Agency's plethora of mission support activities, worked more closely with outside commercial companies to develop new equipment and software for use by the NSA, ceased virtually all of its research and development work on obsolete SIGINT collection and processing systems, and overhauled and realigned its strategic funding relationships with its SIGINT partners at home and abroad.[14]

But critics inside and outside the Agency in interviews have described these changes as "superficial" or "window dressing." The critics noted that the

reorganization of the NSA's internal structure did not result in greater efficiency or efficaciousness, especially within the Agency's senior management. There are now at the NSA 100 "super-grade" senior civilian managers trying to run an organization the size of an army corps, which the U.S. Army can run with eight to ten generals. The result, critics contend, is that the NSA's management structure remains bloated and top-heavy. More important, perhaps, a number of Agency insiders believe that Hayden's organizational changes did not resolve the central issue of dealing with the NSA's hide-bound bureaucracy. A recently retired NSA official quipped, "He's just shuffled the cards rather than getting a new pack."[15]

There is also considerable evidence that General Hayden failed in his attempt to reform the Agency's faulty fiscal management practices. NSA insiders believe that the approach of the NSA's senior management in the 1999–2001 time period was to get the money from Congress "while the going was good," then build a modernization package around the money they got, rather than the other way around. This inevitably led to serious clashes between the NSA and the congressional oversight committees. In October 2001 the Senate Armed Services Committee indicated that it intended to "put the brakes" on further spending on the NSA's modernization programs until the NSA "adopt[ed] a more comprehensive acquisition strategy." A committee report stated the "NSA appears to have made only modest progress in the area most important to its future: acquiring the technical ability to operate effectively against the emerging global effort." The Senate report also expressed concern that the "NSA is spending large sums of money on hundreds of in-house development activities, yet it cannot say how or whether these aid modernization." The committee concluded that "more money now, without further reform, will not succeed either."[16] Finally, in July 2003, a clearly frustrated Congress stripped the NSA of its ability to sign contracts with outside businesses, and in the process, transferred control of the NSA's hundreds of millions of dollars of modernization contracts to the Department of Defense to administer until the Agency proved that it could manage these programs in a fiscally responsible manner.[17]

The NSA has also experienced considerable difficulty since 2000 in hiring and retaining sufficient numbers of the technologically oriented engineering and computer science personnel that it needs in order to develop, operate, and maintain the new high-tech SIGINT collection and processing systems that are beginning to come online. In particular, the NSA has had significant trouble recruiting personnel with advanced technology degrees to work at Fort Meade, including systems engineers, software engineers, and program managers versed in computer hardware and software issues.[18] A current serving NSA manager stated the problem simply: "We can't afford to pay these kids anywhere near the amount of money they could get in private industry, much less offer them a decent benefits package or the stock options they would normally receive working for any decent high-tech company in California."[19]

Moreover, intelligence production at the NSA remained relatively flat in the two years after General Hayden became director, with the quantity of intelligence reporting actually declining in some key areas as money was diverted to

finance research and development work on new high-tech SIGINT collection and processing systems. Available SIGINT collection and analytic resources were gradually shifted away from older "legacy" targets, such as Russia, the former Soviet republics, Cuba, and the Balkans, to new higher priority global intelligence targets, such as international terrorism and nuclear proliferation. General Hayden was forced to admit to a congressional committee looking into the 9/11 intelligence disaster that he felt "handcuffed" in that he was unable to "churn some $200 million into new age signals . . . because we were going to erode our coverage of [other intelligence issues] as part of this effort."[20]

More recently, reports have appeared in the press revealing that not everything has gone according to plan with General Hayden's much ballyhooed multiyear, multi-billion-dollar NSA transformation and modernization effort. Two recent articles in the *Baltimore Sun* have revealed that the two key components of the NSA's modernization program, designated Groundbreaker and Trailblazer, as well as many of their supporting systems, are years behind schedule and hundreds of millions of dollars over budget.[21]

Both projects began relatively well. Initiated with much public fanfare in 1999, Project Groundbreaker was a ten-year, $2 billion program to completely rebuild and modernize the NSA's nightmarish internal information technology (IT) infrastructure.[22] One of the many problems the program was supposed to fix was to remedy the fact that the NSA had sixty-eight different e-mail systems, none of which could communicate with each other. This led General Hayden to comment that it took "an act of God" for him to send an e-mail to all of his employees.[23]

But the centerpiece of General Hayden's modernization effort was a massive overhaul of the NSA's deeply troubled SIGINT collection and processing infrastructure. In January 2000 NSA Deputy Director for Operations, Richard Taylor, proposed a massive reorganization of the NSA's huge Operations Directorate that was designed to refocus the organization on its core mission, SIGINT collection, processing, analysis, and reporting. In addition to putting "our customers squarely front and center in our production process," Taylor proposed reorganizing the Operations Directorate into three functional SIGINT organizations: Collection, Exploitation, and Production, as well as the creation of an Advanced Analytic Techniques organization to "develop and spread the art of analysis." Taylor's proposal also called for removing from the directorate all nonmission functions, such as information technology, policy, budget, and logistics, as well as integrating more military support functions into all of the directorate's functional groups.[24]

The result of Taylor's proposal was the initiation of a highly ambitious program called Project Trailblazer. In January 2000 the NSA announced the initiation of the first phase of its SIGINT processing, analysis, and reporting modernization effort, called Project Trailblazer. According to an internal NSA document, the first phase of Trailblazer was supposed to "deliver tomorrow's analytic tools and functions to automate desktop processing and improve COMINT [communications intelligence] production. It will also provide us with the ability to profile customers' needs and requirements, and will modernize the dissemination process."[25] The

classified objective of the Trailblazer program was to build an integrated series of state-of-the-art SIGINT collection and processing systems that would give the NSA the ability to eavesdrop on communications traffic being carried by e-mail, fiber-optic cable, and cellular telephone systems around the world.[26]

The core focus of the first phase of Trailblazer was to design and build a system to attack the new global SIGINT target environment, which the NSA designated Digital Network Intelligence (DNI). The NSA defined DNI as "the intelligence from intercepted digital data communications transmitted between, or resident on, networked computers."[27] Trailblazer was to form the foundation for this attack by mapping "detailed Digital Network Exploitation (DNE) mission requirements to our cryptologic architecture and provide implementation focus. . . . Trailblazer 1 will build the SIGINT system we would want to build—if today's system didn't exist—to attack a tough, evolving DNE target." Among the different technologies being developed under Trailblazer were selection and filtering tools for NSA analysts, as well as hardware and software for "improved front-end access, collection, processing, and filtering" using web-based tools and techniques, a process that has become known within the NSA by the moniker "e-SIGINT."[28]

By October 2002, developmental work on the Trailblazer system was sufficiently advanced that the NSA awarded a contractor team headed by San Diego–based Science Applications International Corporation a $282 million contract to build a functional prototype of the system in only twenty-six months. But this was the last the public heard about the system for the next three years, which in retrospect should have been a red flag that things were not progressing as well as they should.[29]

As is usually the case, the warning signs of problems with these two multi-billion-dollar programs were there for all to see. As early as 2000, NSA officials complained both publicly and privately that the Agency's reorganization and modernization plans were developed and constructed within segregated "stovepipes" rather than in an integrated and cohesive fashion. The Agency also suffered from an all-too-apparent lack of competent program management, which impaired its ability to effectively manage the various multi-billion-dollar modernization programs.[30] This problem was exacerbated by heavy turnover amongst senior management personnel, which resulted in a failure to reform the Agency's much-maligned contracting practices. As a result, today senior Pentagon and congressional officials are currently concerned that these programs, and related modernization efforts at the NSA, have not been well managed and may not yield the desired results when finally completed.[31]

THE NSA IN THE POST–9/11 ERA

Declassified documents, congressional reports, and the published record of the 9/11 Commission all indicate that the NSA did not commit any egregious errors in the days and months leading up to the attacks. A congressional

investigative report concluded: "Prior to 11 September 2001, NSA had no specific information indicating the date, time, place, or participants in an attack on the United States."[32] There have, however, been recurring indications received from both retired and current U.S. intelligence officials that substantive problems with the Agency's performance prior to 9/11 have not yet been completely revealed because it involves highly classified information concerning the NSA's "sources and methods."[33]

Like the rest of the U.S. intelligence community, the searing events of 9/11 have dramatically changed the NSA, both for better and for worse. The Agency's budget has been dramatically increased every year since 2001, climbing to about $5 billion per annum.[34] NSA manpower has also been shooting upwards at a forty-five-degree angle, with the NSA hiring 3,500 new civilian staff between 2002 and 2004 alone, which raised NSA manpower to about 35,000 military and civilian personnel. Press reports and interviews indicate the NSA intends to hire 12,000 additional civilian personnel between 2004 and 2011, bringing NSA manpower up to more than 40,000 military and civilian personnel by the end of the decade, after retirements and normal personnel attrition are factored in.[35] Moreover, the size of the entire U.S. Cryptologic System, including SIGINT personnel assigned to the CIA, the National Reconnaissance Office, and the military services, has grown to more than 60,000 military and civilian personnel since 9/11, making it by far the single largest component of the U.S. intelligence community. The NSA is in the process of opening new operations centers in San Antonio, Texas, Denver, Colorado, and Salt Lake City, Utah, which when completed will employ several thousand civilian and military staff.[36] In February 2006 Congress passed an emergency supplemental appropriations bill, which included $35 million to immediately expand the NSA's huge listening post at Menwith Hill in northern England, as well as another $700 million to construct new operational facilities at the Agency's large intelligence collection stations at Kunia, Hawaii, and Fort Gordon, Georgia.[37]

But despite the massive budget increases and unfettered operational discretion granted to the Agency since 9/11, the NSA still is not functioning as smoothly or efficiently as it should be. Senior U.S. intelligence officials believe that one of the signature results of the chaos produced by 9/11 is that the NSA, in its rush to respond to the Al Qaeda terrorist attacks on the United States, literally threw away its previous management reform plans. Critics of the Agency within the U.S. intelligence community point to the fact that since 9/11, the size of the NSA's multilayered bureaucracy has once again begun to mount, with a resulting decrease in operational efficiency caused by the retrenchment of stifling bureaucratic practices and procedures at the top levels of the Agency's management. The NSA has also been hurt by the loss of a number of veteran senior officials, who have either retired or quit the Agency in the past two years to take higher paying jobs in the business world.[38] The result, according to the officials, is that in the five years since 9/11 the NSA's relative effectiveness and efficiency have declined noticeably. In fact, interviews with senior intelligence officials suggests

that the NSA's operational performance has declined somewhat in recent years, with officials pointing in particular to the Agency's disappointing performance to date in Afghanistan and Iraq, which is described in greater detail below.[39]

There is also evidence that NSA attempts to balance its spending between maintaining current SIGINT collection operations and at the same time developing new signals collection technologies for the 21st century have not gone well. In some instances since 2001, NSA SIGINT operations have suffered for lack of investment because available fiscal resources were being directed toward research and development on new technologies needed to allow the NSA to intercept and process signals in the new digital environment. But as noted above, the NSA's Groundbreaker and Trailblazer multi-billion-dollar modernization programs have not been effectively managed. Former NSA officials point to the fact that immediately after 9/11 the Agency abandoned a patient, long-term approach to modernization in favor of dubious, short-term "quick-fixes" that have only compounded the host of existing problems with the NSA's various multi-billion-dollar modernization programs.[40] Compounding these internal problems is the massive technological hurdles that the NSA has had to leap through over the past five years trying to develop and build the new high-tech equipment it needs to do its job. Much of the technology that the NSA desperately needs, such as powerful analytic software that is required to help NSA analysts sift through the immense amounts of data being intercepted every day by the Agency's listening posts, just does not exist today on the open market, which has meant that the NSA has had to spend hundreds of millions of dollars developing these systems in-house, and not always successfully.[41]

Moreover, the NSA was forced to make significant changes in its intelligence targeting in order to devote a substantial portion of its intelligence collection resources to the so-called global war on terrorism. This has forced the NSA to give short shrift to many previously important intelligence targets, such as the former Soviet Union, China, North Korea, Bosnia, and the national narcotics interdiction program. The same thing has happened in England. The British Parliament's Intelligence and Security Committee in its June 2003 annual report warned that the shift of precious intelligence collection resources from other targets to counterterrorism was creating a dangerous situation, stating: "These reductions are causing intelligence gaps to develop, which may mean over time unacceptable risks will arise in terms of safeguarding national security and in the prevention and detecting of Serious Organised Crime."[42] Sources note that the NSA's inability to dedicate sufficient resources to monitoring narcotics trafficking in the western hemisphere has forced the Drug Enforcement Administration (DEA)'s small SIGINT organization to largely take over this responsibility.[43] The increasingly important role of the DEA, the CIA, and the military services in the SIGINT field has led, in turn, to the diminishment of NSA control over the national SIGINT effort. The result has been that the NSA has lost somewhat the all-important "centrality of command" that it once enjoyed over the national SIGINT effort.

Interviews with intelligence officials in Washington suggest that the NSA has improved somewhat its customer relations with its consumers in Washington and elsewhere around the globe since 9/11. But apparently not everyone is happy. NSA officials contend that over the past five years its ever-increasing number of customers in Washington have submitted conflicting requirements on the NSA, which has required years of oftentimes contentious negotiations in order to resolve the differing requirements levied on the agency. Interviews with intelligence officials reveal that there are still widespread complaints about the NSA's inability or unwillingness to share information with other government agencies. In particular, FBI officials complain about the lack of cooperation that they have received from the NSA since 9/11. The single largest barrier to the free flow of intelligence information appears to be the compartmentalized nature of the NSA itself, which has prevented an integrated approach to customer relations between the NSA and the rest of the U.S. intelligence community.[44]

THE NEW GLOBAL BATTLEFIELD

The NSA found that its ability to effectively contribute to the global counterterrorism fight and concurrently support U.S. military forces in Afghanistan, which the United States invaded in November 2001, were hampered by the fact that it was not equipped to deal with unconventional intelligence targets operating in the less-developed countries of the world who typically do not use, much less own, computers connected to the Internet, cell phones, personal pagers, and digital assistants, such as the ubiquitous Blackberry, or even an iPod. One recent press report perhaps said it best that SIGINT today "is far less vital against an enemy that sleeps in caves and cellars, and communicates in whispers."[45] Moreover, the NSA's ability to collecting SIGINT in Afghanistan was an extremely difficult proposition given the almost complete lack of linguists at the Agency who could speak the languages spoken in the country.[46] As of fall 2001, the NSA reportedly only had four linguists fluent in the languages spoken in Afghanistan (Pashto, Dari, Uzbek, and Turkmen), including only one who spoke Pashto, the primary language spoken in Pakistan and Afghanistan.[47]

In other words, the Agency's heavy investment in its multi-billion-dollar high-tech modernization efforts of the late 1990s, although badly needed, sadly may have left the NSA prepared to fight the "wrong war" in the 21st century. In fall 2001 chagrined U.S. intelligence officials discovered that the NSA's newly developed high-tech collection systems, which were designed to cover cellular telephones, the Internet, and communications traffic carried on fiber-optic cables, were largely worthless in the low-tech environment of Afghanistan and in northern Pakistan, where the remaining elements of Al Qaeda and their Taliban supporters operated.[48]

The NSA's underwhelming performance on the battlefield led to numerous complaints from the U.S. military services about the Agency's inability to

provide adequate tactical SIGINT support to American military commanders in Afghanistan and to Special Operations Forces engaged in trying to hunt down terrorists in Pakistan and elsewhere around the world. Prior to 9/11 the U.S. Army had denuded its tactical SIGINT collection resources to practically nothing in the mistaken belief that such units were no longer needed in the post–Cold War geostrategic environment. The NSA's failure led the military services, especially the U.S. Army, to allocate over the past five years greater resources to building up their own dedicated tactical SIGINT collection resources that are largely independent of the NSA. As a result, U.S. Army SIGINT assets have now replaced the NSA in Afghanistan.

Over the past three years, U.S. military SIGINT assets in Afghanistan have been gradually reconfigured in order to work more efficiently in the extremely difficult Afghan environment, and more mobile and flexible SIGINT collection and processing systems have been added in recent years.[49] On the plus side of the equation, SIGINT has confirmed that former Taliban commanders based in the tribal areas of northern Pakistan have been orchestrating insurgent attacks against U.S. and Afghan forces in southern and southeastern Afghanistan using satellite phones.[50] SIGINT has also been used effectively to counter Taliban rocket and mortar fire against U.S. military bases in southern and southeastern Afghanistan. By intercepting the walkie-talkie communications traffic of insurgent artillery spotters, U.S. forces have on more than one occasion been able to successfully destroy insurgent rocket and mortar pieces inside Afghanistan, and have forced insurgent forces instead to occasionally fire at outlying U.S. outposts and patrols along the Afghan-Pakistani border without the benefit of spotters inside Afghanistan.[51]

But problems continue to abound in the military's SIGINT collection programs in Afghanistan. Inhibiting the effectiveness of SIGINT in Afghanistan is the fact that the insurgent forces based in northern Pakistan have increasingly moved to the use of couriers and other noninterceptible means of communications rather than radio communications.[52] In addition, persistent shortages of trained linguists have severely hampered the effectiveness of SIGINT in Afghanistan. Since 9/11 the U.S. military has trained at great expense a small number of U.S.-born linguists in the Pashto, Dari, and Urdu dialects to process SIGINT intercepts. But reports from the field indicate that the competency levels of these linguists were so low that they only possessed "the ability to tell the difference between a burro and a burrito."[53] This has meant that the U.S. military today still largely relies on contract employees hired by the Department of Defense to provide U.S. intelligence units and combat units with linguistic capabilities in Urdu, Dari, and Pashto. But according to a 2003 U.S. Army report: "This develops into a big problem, because, not only do you have to have fluent linguists, but you also have to obtain one that can comprehend military terms and operations. . . . Laugh if you will, but many of the linguists with which I conversed were convenience store workers and cab drivers, most over the age of 40. None had any previous military experience."[54] Among the contract linguists hired on an emergency basis for the Department of Defense by Titan Systems Corp., a San

Diego–based defense contractor, were a partner in a San Diego pharmaceuticals company, a software engineer from Texas, and an accountant from northern Virginia, who twenty years earlier had been a commander in the anti-Soviet *mujahedeen* forces.[55]

In addition, the NSA's accomplishments against international terrorist targets have slowed dramatically in recent years after a string of early successes immediately after 9/11. SIGINT's last notable success in the war on terror took place in February 2003, when intercepted e-mails and satellite telephone communications led U.S. and Pakistani security officials to the hideout in the Pakistani city of Rawalpindi of 9/11 mastermind Khalid Shaikh Mohammed. At 4:00 am on March 1, 2003, heavily armed Pakistani security forces burst into Mohammed's hideout and arrested him and another key Al Qaeda operative, Mohammed Ahmed al-Hawsawi, while they slept.[56] But since 2003, SIGINT's successes against international terrorist targets have become fewer and farther between as the surviving members of Al Qaeda and allied terrorist group have learned not to trust electronic communications for communicating with each other. Spying on terrorist organizations is inherently difficult, and the same holds true for SIGINT. Testifying before Congress in 2002, NSA Director General Michael Hayden admitted that "cracking into these targets is hard—very hard—and SIGINT operations require considerable patience—sometimes over years—before they mature."[57]

SIGINT AND THE WAR IN IRAQ

Reviews by both the House and Senate Intelligence Committees in 2004, followed by the Commission on the Capabilities of the United States Regarding Weapons of Mass Destruction (the Robb-Silberman Commission) in 2005, were all highly critical of the NSA's performance in the events leading up to the U.S. invasion of Iraq in March 2003. The NSA fared better than the CIA and the rest of the U.S. intelligence community in these investigations, but only because so much of the criticism of the Agency's performance was withheld from the public versions of these reports because of classification concerns.[58]

What was made public in these reports clearly shows that NSA SIGINT coverage of Iraq prior to the U.S. invasion in March 2003 was poor, especially on the question of whether Iraq was indeed pursuing weapons of mass destruction (WMD) programs. The reason for the NSA's poor performance was that virtually all high-level Iraqi government and military communications traffic was carried by buried fiber-optic cables and thus impervious to NSA radio interceptors. Then on March 18, 2003, only a few days before the invasion began, the Iraqi government switched off all telephone service across Iraq, and the use of satellite and mobile phones was banned by the Iraqi Ministry of the Interior. This closed off the last low-level source of SIGINT then available to the NSA about what was going on inside Iraq.[59]

These factors led a postwar review panel to conclude that for NSA SIGINT collectors "changes in telecommunications technology have brought new challenges. This was the case in Iraq, where the Intelligence Community lost access to important aspects of Iraqi communications."[60] As a result, the panel concluded that insofar as helping the U.S. intelligence community assess the nature and extent of the alleged Iraqi nuclear, chemical, and biological programs, SIGINT "on the whole was not useful."[61] For example, the panel concluded that "Signals Intelligence collection against Iraq's chemical activities was minimal, and much was of questionable value."[62]

What makes these revelations about the NSA's performance so disturbing was the fact that the U.S. government, in attempting to sell its vision of the danger posed by Saddam Hussein's Iraq in Secretary of State Colin Powell's presentation to the UN Security Council on February 5, 2003, depended to a very high degree on evidence obtained from SIGINT provided by the NSA. Powell used three communications intercepts during his February 5, 2003, presentation to the UN Security Council, which unfortunately did not provide tangible "smoking gun" proof for the Bush administration's case that Iraq possessed forbidden weapons of mass destruction.

Adding fuel to concern about the NSA's poor performance in Iraq were the revelations in the press that the NSA had been used by the Bush administration to intensively monitor the communications traffic of those countries or international bodies who opposed the Bush administration's Iraq policies. In January 2003, two months before the U.S.-led invasion of Iraq began, the NSA and GCHQ mounted an intensive effort to monitor the communications traffic of the foreign representatives to the UN Security Council, especially those members of the Security Council who publicly had expressed misgivings about the U.S. government's intentions to invade Iraq. This information was leaked to the press in early March 2003 by a GCHQ employee, who was fired from her job.[63] The NSA was also tasked with monitoring the telephone calls and e-mail communications of Mohamed El Baradei, the head of the United Nation's International Atomic Energy Agency (IAEA), because of the White House's intense dislike of his agency's policies with regard to Iraq, which oftentimes ran counter to what Washington wanted.[64]

Since the invasion of Iraq, NSA performance has been described as being disappointing by senior military commanders who have served there. Military and intelligence officials have confirmed that SIGINT has not been as helpful as it was hoped it would be in tracking down members of the insurgency movement in Iraq. Despite this fact, SIGINT is still the number one source of actionable intelligence on insurgent activities.

Sources confirm that SIGINT has been extremely useful in monitoring the activities of the Iranian and Syrian governments in Iraq. This effort, however, was badly hurt in 2004 by the compromise of these SIGINT efforts by Ahmed Chalabi.[65] Among the major complaints heard from many military officials returning from Iraq is that the NSA has emphasized SIGINT collection coverage

against Iraq's neighbors, Iran and Syria, as well as the internal machinations of the Washington-backed Iraqi government. But SIGINT has not proven to be a meaningful or viable tool for helping root out Iraqi insurgents, who continue to bedevil U.S. and UN Coalition forces in Iraq despite the best efforts of the U.S. intelligence community.

THE NSA DOMESTIC EAVESDROPPING SCANDAL

The NSA currently finds itself at the center of a politically explosive domestic spying scandal that may very well have serious negative consequences for the Agency and the U.S. intelligence community as a whole. In December 2005 the *New York Times* revealed the outlines of the secret NSA eavesdropping program, the purpose of which was to locate Al Qaeda terrorist cells believed to be operating in the United States without referring the matter to the super-secret Foreign Intelligence Surveillance Activity Court for approval.[66]

The controversy over the legality and propriety of this still highly classified program rages on, exacerbated by the fact that neither the House nor the Senate Intelligence Committee has shown much inclination to examine the legal underpinnings of the program, much less ascertain the details of just how the program has been conducted.[67]

The controversy has proven to be particularly embarrassing to the NSA because former NSA Director Lieutenant General Michael V. Hayden told the House Intelligence Committee in April 2000 in no uncertain terms that the Agency did not engage in spying on U.S. citizens, describing this recurring area of concern an "urban myth." He assured the Committee that the NSA would assiduously abide by the legal strictures on such activities as contained in the 1978 Foreign Intelligence Surveillance Act (FISA).[68] In a March 2005 report to President George W. Bush on the U.S. intelligence community's performance against the Iraqi WMD programs, the NSA reported that FISA "ha[d] not posed a serious obstacle to effective intelligence gathering." It should be noted that at the time the NSA made this statement to the review panel the Agency's secret domestic eavesdropping program, which deliberately bypassed the FISA Court, had been ongoing for almost three and a half years.[69] Since the *New York Times* broke the story of the NSA domestic eavesdropping program in December 2005, General Hayden has become the Bush administration's most prominent defender of the legality and probity of the increasingly controversial program, while at the same time declaring publicly that the NSA had strictly abided by the terms of the law barring government spying on Americans. As he stated in a speech at the National Press Club in January 2006: "I've taken an oath to protect and defend the Constitution of the United States. I would never violate that Constitution, nor would I abuse the rights of the American people."[70]

As with all previous scandals involving the NSA, there were portents of what the NSA was up to. In April 2005 a political controversy erupted in Washington

when it was learned that the Bush administration's nominee to be the ambassador to the United Nations, John R. Bolton, had requested from the NSA transcripts of intercepted conversations involving or pertaining to other U.S. government officials. The NSA admitted that it made copies of these transcripts, including the names of the American officials involved, available to Mr. Bolton.[71] A few weeks later, *Newsweek* revealed that since January 2004 the NSA had received between 3,000 and 3,500 requests for transcripts of intercepted communications involving American citizens from various U.S. government departments, 400 of which came from the State Department. The NSA had complied with all of these requests. The report indicated that the names of as many as 10,000 Americans were contained in the transcripts of the intercepts turned over to the various U.S. government agencies who had requested them.[72] It was later learned that Bolton personally had originated ten requests since January 2004 for unredacted NSA intercept transcripts that mentioned the names of U.S. government officials or American citizens.[73]

Since the first article about the domestic eavesdropping program appeared in the *New York Times* in December 2005 further information about the nature and extent of the NSA domestic surveillance program has been slow in coming, but what has been revealed to date suggests that the program may have been far larger and more pervasive than initially indicated in the first press reports. In April 2006, an AT&T technician revealed that the telecommunications giant he worked for had allowed the NSA to place eavesdropping equipment inside its network switching centers in San Francisco and Atlanta, through which much of America and the world's e-mail traffic passes. This may, in fact, be the tip of the iceberg because a number of key American telecommunications companies other than AT&T have plaintively refused to answer questions from reporters about whether they too cooperated with the NSA's domestic eavesdropping effort.[74] These reports, taken together, all clearly indicated that the NSA had crossed the rubicon and was engaged in doing something that it had not done since the days of Henry Kissinger in the late 1960s—give Bush administration officials intelligence products involving intercepted conversations involving U.S. citizens. Unfortunately, the Bush administration refused to turn over to Congress any details concerning these NSA operations, and Mr. Bolton was subsequently confirmed as the U.S. ambassador to the United Nations.

The fear among recently retired and active-serving NSA officers is that the Agency's domestic eavesdropping program, in addition to generating much unwanted negative publicity for the Agency, almost certainly diverted much-needed manpower and fiscal resources from the NSA's foreign intelligence gathering mission to what the Agency officers generally believe to have been a poorly considered and legally questionable domestic monitoring operation that apparently has produced little in the way of tangible results, despite claims to the contrary from the White House. The program has also only served to further exacerbate the NSA's already poor relations with the FBI, which for reasons

passing easy comprehension, was deliberately excluded from participation in the domestic eavesdropping program by the White House.

THE SUM OF ALL ITS PARTS

Today, the NSA remains a conundrum. It is by far the largest and most powerful intelligence agency within the U.S. intelligence community. It is today the principal intelligence collector for the entire U.S. intelligence community, accounting for the majority of the highest-level intelligence information going to the president of the United States.

And yet, like the community of which it is an integral part, it remains deeply troubled by a host of problems, many of its own making. NSA intelligence production, while rising in absolute numbers, has been declining in real terms in key areas, such as its ability to find insurgents in Afghanistan and Iraq. General Hayden's internal reform measures at the NSA were left unfinished, in part because all reform measures were largely abandoned after 9/11. All of the NSA's major technical modernization programs are hundreds of millions of dollars over budget and years behind schedule. It has been left to General Hayden's successor at the helm of the NSA, Lieutenant General Keith Alexander, to try to put the NSA's various internal reform and modernization programs back on track while at the same time increase its productivity and good standing within the U.S. intelligence community.

NOTES

1. NSA/CSS, *Transition 2001*, December 2000, p. 33. The author is grateful to Dr. Jeffrey T. Richelson for making a copy of this document available.

2. David Ignatius, "The CIA at Rock Bottom," *Washington Post*, May 7, 2006, p. B7.

3. A detailed examination of the NSA's Cold War accomplishments and failures against the Soviet Union can be found in Matthew M. Aid, "The National Security Agency and the Cold War," in *Secrets of Signals Intelligence During the Cold War and Beyond,* eds. Matthew M. Aid and Cees Wiebes (London: Frank Cass, 2001), pp. 27–66.

4. Matthew M. Aid, "The Time of Troubles: The U.S. National Security Agency in the Twenty-First Century," *Intelligence and National Security* 15 (Autumn 2000), p. 6. See also *Statement for the Record by Lt. General Michael V. Hayden, USAF, Director NSA/CSS Before the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence*, October 17, 2002, p. 6.

5. Senate Report No. 107-351 and House Report No. 107-792, Report of the U.S. Senate Select Committee and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd Session, December 2002 (declassified and released in July 2003), p. 76.

6. Heritage Lecture #851, Joel F. Brenner, *Information Oversight: Practical Lessons From Foreign Intelligence*, September 30, 2004, the Heritage Foundation, available at http://www.heritage.org/Research/NationalSecurity/hl851.cfm.

7. Michael Hirsh, "The NSA's Overt Problem," *Washington Post*, January 1, 2006, p. B1.

8. This troubled period in the NSA's history is covered in detail in Matthew M. Aid, "The Time of Troubles: The U.S. National Security Agency in the Twenty-First Century," *Intelligence and National Security* 15 (Autumn 2000), pp. 1–32.

9. Vernon Loeb, "General Named to Head NSA," *Washington Post*, February 25, 1999, p. A21; "Agency Welcomes New Director Lieutenant General Michael V. Hayden," *National Security Agency Newsletter*, May 1999, p. 4.

10. Memorandum, Taylor to DIRNSA, *Thoughts on Strategic Issues for the Institution*, April 9, 1999, p. 2, NSA FOIA.

11. Richard Lardner, "NSA Chief Pushes Ahead With Overhaul of Agency's Culture, Operations," *Inside Defense*, October 16, 2000; Vernon Loeb, "NSA's Chief Unveils Restructuring," *Washington Post*, October 17, 2000, p. A31; Laura Sullivan, "Chief of NSA Begins Reforms," *Baltimore Sun*, October 17, 2000.

12. Confidential interview.

13. Vernon Loeb, "NSA Reorganization," *Washington Post*, December 19, 2000, p. A37.

14. NSA/CSS, *Transition 2001*, December 2000, p. 19.

15. Confidential interview.

16. Frank Tiboni, "Bill Calls for Pentagon to Monitor Spy Shop's Spending," *Defense News*, October 1–7, 2001, p. 6.

17. Ariel Sabar, "Congress Curbs NSA's Power to Contract With Suppliers," *Baltimore Sun*, July 20, 2003, p. A1.

18. Thomas R. Temin, "Defense Coders Are Fading Away," *Government Computer News*, May 6, 2002.

19. Confidential interview.

20. Senate Report No. 107-351 and House Report No. 107-792, Report of the U.S. Senate Select Committee and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd Session, December 2002 (declassified and released in July 2003), p. 381.

21. Siobhan Gorman, "System Error," *Baltimore Sun*, January 29, 2006, p. A1; Siobhan Gorman, "Computer Ills Hinder NSA," *Baltimore Sun*, February 26, 2006, p. A1.

22. DIRgram-31: "Fixing NSA's IT Infrastructure," January 6, 2000, NSA FOIA.

23. Neil King Jr., "Big Technology Players Vie to Upgrade NSA Computers," *Wall Street Journal*, March 13, 2001.

24. DIRgram-42, "DO Realignment and Transformation," January 24, 2000, NSA FOIA.

25. DIRgram-37: "Transformation Begins With TRAILBLAZER," January 14, 2000, NSA FOIA.

26. Confidential interview.

27. NSA Scientific Advisory Board, Panel on Digital Network Intelligence (DNI), *Report to Director*, June 28, 1999, p. 20/61. The author is grateful to Dr. Jeffrey T. Richelson for making a copy of this document available.

28. DIRgram-45: "TRAILBLAZER I—A Progress report," February 3, 2000, NSA FOIA.

29. SAIC Press Release, *SAIC Team Wins National Security Agency TRAILBLAZER Contract*, October 21, 2002; Frank Tiboni, "NSA to Boost Range of Cryptologic Capabilities; Earmarks $282 Million for Eavesdropping Network," *Defense News*, January 20, 2003.

30. Senate Report No. 107-351 and House Report No. 107-792, Report of the U.S. Senate Select Committee and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd Session, December 2002 (declassified and released in July 2003), p. 76.

31. Confidential interviews.

32. Senate Report No. 107-351 and House Report No. 107-792, Report of the U.S. Senate Select Committee and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd Session, December 2002 (declassified and released in July 2003), p. 374.

33. For an assessment of NSA's performance prior to 9/11, see Matthew M. Aid, "All Glory Is Fleeting: Sigint and the Fight Against International Terrorism," *Intelligence and National Security* 18 (Winter 2003), pp. 72–120.

34. Confidential interview.

35. Ariel Sabar, "Want to Be a Spy? NSA Is Hiring," *Baltimore Sun*, April 10, 2004; Stephen Barr, "NSA Makes No Secret of Stepped-Up Recruitment Effort," *Washington Post*, April 22, 2004, p. B2; "A Good Spy Is Hard to Fund," *U.S. News & World Report*, November 22, 2004.

36. Sheila Hotchkin, "NSA Will Let Its Dollars Do the Talking," *San Antonio Express-News*, April 16, 2005; Mike Soraghan and Aldo Svaldi, "NSA Moving Some Workers, Operations to Denver Area," *Denver Post*, January 24, 2006; Robert Gehrke, "Key Spy Agency Expands to Utah," *Salt Lake Tribune*, February 2, 2006; Amy Choate, "NSA Seeks Linguists at BYU to Staff Utah Center," *Deseret Morning News*, February 24, 2006.

37. "Emergency War Supplemental Hides Millions," *UPI*, February 20, 2006.

38. Confidential interview.

39. Confidential interviews.

40. Michael A. Wertheimer, "Crippling Innovation—and Intelligence," *Washington Post*, July 21, 2004, p. A19.

41. Joab Jackson, "NSA Seeks Better Analysis Technologies," *Washington Technology*, November 11, 2004, available at http://www.wtonline.com.

42. CM 5837, Intelligence and Security Committee, *Annual Report 2002–2003*, June 2003, p. 20.

43. Confidential interview.

44. Memorandum, Zenker to Joint Tactical SIGINT Architecture (JTSA) Working Group, *Quarterly Meeting Minutes—December 2001*, December 31, 2001. This document has since been reclassified and removed from the Internet site where the author originally found it.

45. Robert Little, "NSA Methods Lag in Age of Terror," *Baltimore Sun*, December 9, 2004.

46. Senate Report No. 107-351 and House Report No. 107-792, Report of the U.S. Senate Select Committee and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd Session, December 2002 (declassified and released in July 2003), p. 336.

47. Ian Bruce, "Mistake in Translation Almost Proves Deadly," *Scotland Herald*, April 24, 2002.

48. Confidential interviews.

49. John L. Girardeau, "TSM Notes—Changes in Tactical Signals Intelligence and Electronic Warfare Forces During Operation Enduring Freedom," *Military Intelligence Professional Bulletin*, October–December 2003.

50. Paul Haven, "Taliban Plans Attacks From Pakistan," *Associated Press*, September 23, 2003.

51. Department of the Army, Center for Army Lessons Learned (CALL), *Newsletter No. 03-27: Project OUTREACH: Tactics, Techniques, and Procedures*, October 2003, p. 19.

52. B. Raman, "Sons' Killings Change Little in Iraq,"*Asia Times Online*, July 31, 2003, available at http://www.atimes.com/atimes/Middle_East/EG31Ak03.html.

53. Department of the Army, Center for Army Lessons Learned (CALL), *Newsletter No. 03-27: Project OUTREACH: Tactics, Techniques, and Procedures*, October 2003, p. 12.

54. Department of the Army, Center for Army Lessons Learned (CALL), *Newsletter No. 03-27: Project OUTREACH: Tactics, Techniques, and Procedures*, October 2003, p. 12.

55. Greg Miller, "Shortage of Linguists Initially Hampered U.S. Intelligence Mission," *Los Angeles Times*, July 28, 2002.

56. Kevin Johnson and Jack Kelly, "Terror Arrest Triggers Mad Scrammble," *USA Today*, March 2, 2003; Rory McCarthy and Jason Burke, "Endgame in the Desert of Death for the World's Most Wanted Man," *Observer*, March 9, 2003; Kevin Whitelaw, "A Tightening Noose," *U.S. News & World Report*, March 17, 2003.

57. Senate Report No. 107-351 and House Report No. 107-792, Report of the U.S. Senate Select Committee and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd Session, December 2002 (declassified and released in July 2003), p. 380.

58. All information concerning the NSA's performance in the Iraqi WMD scandal was deleted from the report of the Senate Intelligence Committee on the U.S. intelligence community's performance prior to the invasion of Iraq, for which see: U.S. Senate, Select Committee on Intelligence, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*, 108th Congress, July 7, 2004, pp. 264–65.

59. "Iraq Shuts Down Phone Network to Thwart CIA Eavesdropping," *Associated Press*, March 19, 2003.

60. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005, pp. 15, 163–64.

61. Ibid., p. 65.

62. Ibid., p. 130.

63. Martin Bright, Ed Vulliamy, and Peter Beaumont, "Revealed: U.S. Dirty Tricks to Win Vote on Iraq War," *Observer*, March 2, 2003, p. 1.

64. Dafna Linzer, "IAEA Leader's Phone Tapped," *Washington Post*, December 12, 2004, p. A1.

65. Rupert Cornwell, "Chalabi Falls From Grace as U.S. Spy Row Erupts," *Independent*, June 3, 2004, p. A1.

66. James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005, p. A1; Eric Lichtblau and James Risen, "Eavesdropping Effort Began Soon After Sept. 11 Attacks," *New York Times*, December 18, 2005, p. A1.

67. See, for example, the heated words exchanged between Republican and Democratic members of the House Intelligence Committee about the NSA's domestic eavesdropping program contained in U.S. House of Representatives, Report 109-411, *Intelligence Authorization Act for Fiscal Year 2007*, 109th Congress, 2nd Session, April 6, 2006.

68. *Statement for the Record of NSA Director Lt. General Michael V. Hayden, USAF Before the House Permanent Select Committee on Intelligence*, April 12, 2000. General Hayden's "urban myth" comment is contained in Neil King Jr., "U.S. Security Agency Defends Eavesdrop Use," *Wall Street Journal*, April 13, 2000.

69. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005, p. 375.

70. Scott Shane and Mark Mazzetti, "Top C.I.A. Pick Has Credentials and Skeptics," *New York Times*, May 6, 2006, p. A1.

71. Douglas Jehl, "Senator Asks U.N. Nominee to Explain His Security Requests," *New York Times*, April 14, 2005, p. A1.

72. Mark Hosenball, "Periscope: Spying—Giving Out U.S. Names," *Newsweek*, May 2, 2005.

73. Katherine Shrader, "Bolton Requested 10 Names in Spy Reports," *Associated Press*, June 27, 2005.

74. John Markoff and Scott Shane, "Documents Show Link Between AT&T and Agency in Eavesdropping Case," *New York Times*, April 13, 2006, p. A1.

4

INTELLIGENCE

The Imagery Dimension

JEFFREY T. RICHELSON

THE USE OF OVERHEAD PLATFORMS TO OBSERVE events on the earth has a long history. According to Chinese and Japanese folklore, spotters ascended in baskets suspended from giant kites or were strapped directly onto them. In April 1794, in the midst of the French Revolution, France organized a company of *aerostiers*, or balloonists. One balloon is said to have been kept in the air for nine hours while the group's commander made continuous observations during the Battle of Fleurus in Belgium.[1]

The United States made similar use of balloons during the Civil War, although little intelligence of value was obtained. By the latter part of the 19th century, Britain was conducting experiments using balloons as platforms from which to obtain "overhead photography."

As a result of Wilbur and Orville Wright's invention of the airplane in 1903, a faster moving reconnaissance platform became available. In January 1911 the San Diego waterfront became the first target of cameras carried aboard an airplane. Between 1913 and 1915 visual and photographic reconnaissance missions were flown by the U.S. Army in the Philippines and along the Mexican border. During World War II the United States made extensive use of airplane photography using remodeled B-17 (*Flying Fortress*) and B-24 (*Liberator*) aircraft. The remodeled B-24, known as the F-7, carried six cameras internally—all triggered via remote control by an operator over the sealed rear bomb-bay doors.[2]

The United States was far from the only nation, in the first half of the 20th century, conducting extensive photographic reconnaissance using airplanes. During World War I British and German aircraft spied on developments on the battlefield. Aerial photography played a significant role in July 1916 in alerting German forces of the impending British attack that launched the Battle of the

Somme. In the interwar years, Britain conducted covert overflights of Germany by hiding cameras on what appeared to be a civilian aircraft, while German aircraft brought back photographs of Soviet territory prior to the German invasion of the Soviet Union in June 1941. Once war arrived, British and American planes photographed German military and industrial installations and areas on a regular basis—to aid in targeting and damage assessment.[3]

The end of World War II was quickly followed by the Cold War and overhead reconnaissance retained, and even increased, its importance—particularly for the United States and its allies, as they sought to pierce the veil of secrecy wrapped around almost every aspect of Soviet life, particularly its military capabilities. At first Cold War aerial reconnaissance was conducted with aircraft, and occasionally with balloons. The possibility that a satellite could be outfitted with a camera to take pictures of any target on earth was noted by the RAND Corporation as early as 1946. In August 1960 that vision was realized when the United States successfully orbited a camera-carrying satellite code-named CORONA.

During the Cold War era, while a multitude of countries used aircraft to obtain overhead images, only the United States, the Soviet Union, and (occasionally) China operated satellites capable of returning the high-quality images needed to extract significant intelligence. Today, though there are still a multitude of nations operating reconnaissance aircraft, there has been a significant proliferation in the nations who also rely on space reconnaissance to provide intelligence. In addition, over the years there has also been an evolution with regard to the different means by which images could be obtained and transmitted.

IMAGERY: VARIETIES AND QUALITY

At one time, the only means of producing an image of a target was through photography. But today, the visible-light portion of the electromagnetic spectrum is not the only segment of the spectrum that is employed to obtain an image. And there are alternative means for converting the signals from portions of the spectrum into images.

Equipment used to produce photographs can be film-based or electro-optical. A conventional camera captures a scene on film by recording the varying light levels reflected from all of the separate objects in the scene. In contrast, an electro-optical camera converts the varying light levels into electrical signals. A numerical value, from 1 to 256, is assigned to each of the signals, which are called picture elements, or pixels. The process transforms a picture (analog) image to a digital image that can be transmitted electronically to distant points. The signal can then be reconstructed from the digital to the analog format. The analog signal can be displayed on a video screen or made into a photograph.

In addition to the visible-light portion of the electromagnetic spectrum, the near-infrared portion of the spectrum, which is invisible to the human eye, can be employed to produce images. At the same time, near-infrared, like visible-light

imagery, depends on objects reflecting solar radiation rather than on their emission of radiation. As a result, such imagery can be produced only in daylight and in the absence of substantial cloud cover.

Thermal infrared imagery, obtained from the mid- and far-infrared portions of the electromagnetic spectrum, provides imagery purely by detecting the heat emitted by objects. Thus, a thermal infrared system can detect buried structures, such as missile silos or underground construction, as a result of the heat they generate. Since thermal infrared imagery does not require visible light, it can be obtained under conditions of darkness—if the sky is free of cloud cover.

Imagery can be obtained during day or night in the presence of cloud cover by employing an imaging radar (an acronym for *ra*dio *d*etection *a*nd *r*anging). Radar imagery is produced by bouncing radio waves off an area or an object and using the reflected returns to produce an image of the target. Because radio waves are not attenuated by the water vapor in the atmosphere, they are able to penetrate cloud cover.

The ultimate utility of any imaging system is a function of several factors—the most important being spatial resolution. A simple measure of resolution is the minimum size an object must be in order to be measurable and detectable by imagery interpreters. The higher the resolution (the smaller the size an object can be and be detected), the greater the detail that can be extracted from an image. It should also be noted that resolution is the product of a number of factors—including the quality of the imaging system itself, atmospheric conditions, contrast, and orbital parameters. Thus, the quality of images from the same imaging system will vary depending on whether the image is obtained on a crisp, clear day or a hazy one, on whether a dark (light) target is being imaged against a light (dark) background, and whether the target is imaged from a lower or higher altitude.

The degree of resolution required depends on the specificity of the intelligence desired. Five different interpretation tasks have been differentiated. *Detection* involves locating a class of units or objects or an activity of interest. *General identification* involves determining a general target type, and *precise identification* involves discrimination within target types. *Description* involves specifying the size-dimension, configuration-layout, components-construction, and number of units. Technical intelligence involves determining the specific characteristics and performance capabilities of weapons and equipment.

SATELLITE IMAGERY

The United States pioneered, in a number of ways, the use of satellites to obtain images to satisfy intelligence requirements. It orbited the first satellite to return images—the previously mentioned CORONA. It also pioneered the use of infrared and radar imagery in spy satellites, as well as dramatically altering the means of transmitting the imagery back to earth. The present U.S. constellation of imagery satellites is a reflection of those developments.

On December 19, 1976, the first of a new generation of U.S. imagery satellites was launched from Vandenberg Air Force Base into an orbit that took it as close as 164 miles to the earth and as far as 329 miles away. Another seven would be launched successfully, before they would begin being replaced by a significantly upgraded version in 1988. By that time, that group of satellites was capable of producing images with 6-inch resolution or better.[4]

The KH-11 represented a quantum leap in imagery capabilities because, in contrast to its film return predecessors, it could return its imagery in "near real-time." Its electro-optical system, employing light-sensitive silicone diodes and charged couple devices, converted images into electronic signals that were transmitted to relay satellites and back to a ground station in northern Virginia for near-instantaneous reconstruction.

The satellites flew lengthwise, with the axis of the optical system parallel to the earth. The inclination of the satellites, approximately 97 degrees, meant they flew in a sun-synchronous orbit, so that the sun angle was the same each time the satellite was over a target. In the front was a downward-looking mirror that could be flipped from side to side, allowing the area under observation to be changed from moment to moment. Two benefits resulted from that capability. One was that the menu of targets included not only areas under the spacecraft but areas to the sides and for hundreds of miles in front. In addition to expanding the intelligence community's ability to monitor a given target, it complicated foreign denial and deception activities. In addition, it permitted the production of stereoscopic images.

The advanced KH-11 can carry more fuel than the original model, perhaps 10,000 to 15,000 pounds. This permits a longer lifetime for the new model—possibly up to eight years. A greater fuel supply also allows a greater ability to maneuver. Thus, an advanced KH-11 can operate at times in higher orbits to produce images covering a larger territory than is possible at lower altitudes—and then maneuver to lower orbits to produce higher resolution imagery. The maneuvering capability could be employed in attempts to evade anti-satellite (ASAT) weapons or to defeat denial and deception activities.

In addition to the ability to operate in higher orbits these satellites have other capabilities. They contain an infrared imagery capability, including a thermal infrared imagery capability, thus permitting imagery during darkness. The satellites also carry a system that places the necessary markings on returned imagery to permit its full exploitation for mapping purposes. At the present, three advanced KH-11 satellites constitute a full constellation.

As might be expected, those satellites have imaged a wide variety of targets, including a nuclear reactor in Algeria, intermediate-range ballistic missile complexes in China, a Russian signals intelligence facility in Cuba, the Pokhran nuclear test site in India, suspected weapons of mass destruction facilities in Iraq, tunnel construction in North Korea, an underground command bunker in Russia, refugee movements in Rwanda, and an aircraft carrier in the Ukraine.

A second component of the U.S. space imaging fleet is satellites developed and deployed under a program first known as Indigo, then as Lacrosse, and more

recently as Onyx. Rather than employing an electro-optical system, they carry an imaging radar. Though the United States had launched a single radar-imagery satellite in 1964, designated Quill, it had not followed that launch with others—despite the mission's success. Thus, the next radar-imagery satellite would be the first Lacrosse, launched on December 2, 1988, from the space shuttle orbiter *Atlantis*. The satellites closed a major gap in U.S. capabilities by allowing the U.S. intelligence community to obtain imagery even when targets were covered by clouds. Further launches have allowed the United States to maintain two radar-imagery satellites in orbit. The satellites have operated in orbits of approximately 400 miles and have a resolution of 3 to 5 feet, reportedly sufficient to allow discrimination between tanks and armored personnel carriers and identification of bomb craters of 6 to 10 feet in diameter.[5]

When conceived, the primary purpose envisioned for the satellite was monitoring Soviet and Warsaw Pact armor. Recent missions have included providing imagery for bomb damage assessments of the consequences of Navy Tomahawk missile attacks on Iraqi air defense installations in September 1996; monitoring Iraqi weapons storage sites; and tracking Iraqi troop movements, such as the dispersal of the Republican Guard when the Guard was threatened with U.S. attack in early 1998. The satellites may also have been used to determine if submarines operating underwater could be located and tracked via radar imagery.

The United States also operates a stealth satellite, originally known at Misty, which returns electro-optical imagery. Designed to be less detectible than other U.S. satellites by space surveillance systems—due to its design and being operated in an unusual orbit for an imaging satellite—the first version was launched in 1990 and another in 1999.

The Soviet Union trailed the United States in the development of reconnaissance satellites but they still represented a key part of Soviet intelligence capabilities until the collapse of the regime. The first Soviet experimental photographic reconnaissance satellite was launched in April 1962, and the first fully operational satellite in 1964. By the end of 1983 the number of days each year in which a Soviet photo reconnaissance satellite was in orbit was approaching 365. Then in 1984, about seven years after the United States accomplished the feat, the Soviets orbited their first real-time imagery satellite.

As did the United States, the Soviet Union employed its satellites for more than monitoring its main adversary's homeland. Its satellites photographed developments in the 1967 Arab-Israeli war, the Indo-Pakistani war of 1971, the 1973 Yom Kippur War, South Africa's apparent preparations for a nuclear test in 1977, the Iran-Iraq war, the 1983 U.S. invasion of Grenada, and, almost surely, the UN invasion of Iraq in 1991. Since then Russian satellites have undoubtedly monitored terrorist activities in Chechnya, nuclear developments in Iran, as well as U.S. military operations in Iraq.

In the Cold War era space reconnaissance was almost exclusively an activity conducted by the superpowers. Aside from China, whose spy satellite program for a number of years consisted of a single, brief, yearly mission, the only other

nations to operate such satellites were the United States and the Soviet Union. But the end of the Cold War has seen a proliferation in satellite reconnaissance operations in countries that previously had to rely on aerial reconnaissance, commercial observation satellites, or the willingness of the United States to share either imagery or intelligence derived from the imagery.

Though such systems represent a significant commitment in terms of technical resources, manpower, and money, several nations have clearly been attracted by both the technical advantages (discussed below) as well as the political advantages. Such nations can reduce their dependency on the United States, be certain of being able to obtain imagery when they deem it important, and have an asset they can trade—because their satellites would be able to supplement U.S. coverage in a crisis.

Israel was the first nation to join the post–Cold War space reconnaissance club, when its third Ofeq (Horizon) satellite was launched in early April 1995. In contrast to other nation's reconnaissance satellites, which operated in polar orbits that allowed them to photograph almost any point on the earth, Ofeq-3 operated in an orbit that limited its view to targets between 37 degrees north latitude and 37 degrees south latitude—which meant that the satellite would spend more time over important Middle East targets. The most recent version of Ofeq, launched in 2002, is reported to have a resolution of between 1.6 and 2.6 feet.[6]

Within months France followed Israel. As early as 1965, France had contemplated building such a spacecraft, but it was not until an Ariane booster lifted off from a launch site in French Guiana in July 1995 and placed Helios 1A in orbit that France actually attained such a capability. Though the reported resolution of the electro-optical satellite was about 3.25 feet—significantly inferior to that produced by U.S. and Russian satellites—it was a considerable improvement over what could be obtained, at that time, from a commercial observation satellite.

Over the next decade France continued to launch Helios satellites. In December 1999 it orbited Helios 1B, and in December 2004, Helios 2A was launched into a 400-mile orbit. The new satellite, partially funded by Spain and Belgium, was a significantly improved version of the earlier generation in several ways. Its imaging quality is estimated to be less than 1.6 feet. In addition, it carries an infrared sensor. It can also deliver about a hundred images a day, in contrast to the dozens that were returned by Helios 1A.

France's commitment to develop Helios, after a number of false starts in earlier decades, was a product of the 1991 Gulf War—which demonstrated the nation's extreme dependence on U.S. satellite imagery. In the case of Japan, it was the August 31, 1998, launch of a North Korean Taepodong missile that convinced Japanese leaders that Japan needed its own spy satellite rather than continuing to debate whether Japan should develop such a system—for warning of the launch came from the United States and not as quickly as the Japanese leadership would have liked. Less than five years after the North Korean launch, in March 2003, Japan orbited two spy satellites, whose names—Optical-1 and Radar-1—also revealed the sensors on board.

All the nations currently operating imaging satellites plan to continue the practice and improve their capabilities. Japan is planning to increase the size of its reconnaissance constellation as well as to improve the resolution of the satellites. Israel's Ofeq-7 is expected to represent a "quantum leap" over earlier models. In addition, Israel plans to launch a radar imagery demonstration satellite in 2006. And other nations, such as Germany and Italy, plan to join the space reconnaissance club.

The continued commitment to space reconnaissance by the nations currently operating such systems and the intent of others to join the space reconnaissance fraternity is a reflection of the benefits attached to such capabilities. Although operating a small fleet of reconnaissance aircraft is far cheaper, and less challenging technically, it cannot provide the benefits of a space reconnaissance capability.

Possibly the most significant impact of satellite reconnaissance is the access it permits to intelligence targets. The U-2 represented a major improvement over the modified bombers employed for photographic reconnaissance that generally operated on the Soviet periphery and very occasionally overflew Soviet territory. But the entire U-2 aerial reconnaissance program (discussed below) involved only twenty-three successful overflights over a period of almost four years. Further, each of those overflights covered a very small portion of the Soviet Union. Their number and extent were a recognition of the limitations on the U-2's range as well as the perilous nature of overflying Soviet territory. Thus, a July 1960 CIA report noted that "7.5% of [the] total land area of USSR is covered by useable [U-2] photography."[7]

In contrast, even the earliest CORONA missions, with one-day lifetimes, would pass over substantial portions of the U.S.S.R. from the western part of the country to Siberia. Of course, while the shoot-down terminated U-2 access to targets in the Soviet interior, all facilities or activities of interest anywhere in the Soviet Union could, assuming favorable weather conditions, be photographed by satellite. Two potential manmade impediments to access did not materialize in any serious way. The Soviet leadership, although authorizing an extensive antisatellite research and development program, never authorized use of such weapons to impede U.S. reconnaissance satellites. And while the Soviets had a significant denial and deception program, managed by a chief directorate of the Soviet General Staff, U.S. imagery satellites were able to produce vast quantities of hard intelligence.

Imaging satellites also gave the United States an ability to access targets in other denied territories such as China (U-2 overflights of which were halted in 1968) as well as allied or friendly countries, such as Israel, where repeated overflights would represent a significant political problem. Similarly, the nuclear programs of Taiwan and France (particularly its southern Pacific testing facility) could be monitored without resorting to intrusive overhead missions. Thus, the CIA conducted one U-2 overflight of the French testing facility and then decided not to repeat such an activity.[8]

Two other major consequences of satellite reconnaissance were the increased frequency with which targets could be imaged as well as the number of targets that could be covered in a given time span. U-2, SR-71, or other overflight missions, if they could be conducted at all over particular targets, could be conducted only sporadically and for very limited durations due to a wide range of reasons, some interrelated. Cost, the availability of pilots and aircraft, the range of the aircraft, and the risks involved in the missions were all factors. In contrast, satellite imagery systems could stay in orbit for a longer period of time—at first by hours, then by days, then by months, then by years, and maybe now by a decade.

In addition, satellites flew at a far greater speed than aircraft as the spinning earth presented a global array of targets beneath them. As a result, targets could be revisited on a regular basis if there was any requirement to do so and the number of targets that could be imaged in any significant time span by a satellite was far greater than possible for an aircraft. This advantage became even more pronounced as the size of the standard imagery constellation grew. In late 1995, with three electro-optical and two radar imagery satellites in orbit, the United States was able to obtain four images a day of the Indian nuclear test site at a time when it was suspected (correctly) that India was preparing to detonate a nuclear device.

Satellites also provided a higher vantage point than aircraft. As a result, a single image taken from a satellite, with its higher vantage point, can encompass far more territory than that taken from an aircraft. As a result of a superior vantage point, the speed of the satellite and rotation of the earth, its ability to operate for longer periods of time than aircraft, and its unimpeded access to targets, the first CORONA (which completed seventeen orbits of the earth and seven passes over the Soviet Union) mission produced 1,432 photos and covered more territory than all twenty-three U-2 overflights of the Soviet Union combined.[9]

The same considerations, technical and political, hold true today—not only for the United States, but for all other nations operating or planning to operate satellite imagery systems. Thus, Japan can obtain satellite images of North Korea with impunity. Conducting aerial reconnaissance missions would involve violations of international law and eventual major domestic and foreign crises. North Korean protests and attempts (which would eventually succeed) to shoot down a Japanese spy plane would certainly trigger both a political crisis within Japan, and a crisis with North Korea. As a result, such missions would never even be proposed, much less authorized.

Further, even if Japan could fly over North Korean territory with impunity, the cost of obtaining the same level of coverage and maintaining the same probability of detecting North Korean activities of interest (e.g., preparations for a missile launch or a nuclear test) would be far greater than employing satellites. The costs would involve a very large fleet of aircraft, personnel, spare parts, and fuel. And, the same satellites that cover North Korea also photograph Chinese targets.

The same considerations apply to Israel, which can avoid the crises that would result from an aerial reconnaissance mission if the plane was shot down

and the pilot captured on a mission over Syria or Iran, by employing satellite coverage. In the case of France, it would need, among other things, a series of bases around the world to launch reconnaissance aircraft if it wanted to match the reach of its Helios satellites. With Helios, it only needs its base in French Guiana and a ground station.

AERIAL SYSTEMS

Aerial reconnaissance comes in two basic varieties: manned and unmanned. Nations, even those who have developed advanced space reconnaissance capabilities, have also continued to operate aerial reconnaissance systems.

Providing a hedge against the unexpected failure of one of its limited number of satellites is one reason for a nation to continue to operate such systems. But there are others. They can supplement satellite coverage—a single plane costs far less than an additional satellite. They can provide a quick reaction capability because an aircraft can head directly for a target whereas a satellite cannot photograph a target until its orbit and the rotation of the earth place the target in view—a process which can take several days. Those same constraints mean that a satellite cannot arbitrarily cover any stretch of territory desired, but aircraft can cover the territory between any two points—for example, the movement of an invading army toward its objective or the movement of refugees toward a border.

The initial development and improving capabilities of imagery satellites has not made other forms of overhead imagery collection obsolete. During the early days of the Cold War, U.S. Air Force pilots flew modified bombers, equipped with cameras, along the periphery of the Soviet Union and China to obtain imagery of airfields, ports, and other facilities that could be photographed from outside those nations' borders. Occasionally, those modified bombers were sent into Soviet airspace to obtain imagery of targets farther inland.

Then in 1956 the CIA pilots began flying deep into the Soviet territory, employing the specially designed U-2, which flew at over 65,000 feet and which the CIA believed, incorrectly, would not be detected by Soviet radar. It carried a special, long, focal-length camera capable of photographing objects as small as a man, and brought back images of roads, railroads, industrial plants, nuclear facilities, aircraft, and missile sites within a strip 200 miles wide by 2,500 miles long.[10]

Overflights of the Soviet Union ceased after Francis Gary Powers and his U-2 were shot down on May 1, 1960. But the United States still continues to operate U-2s, and has employed a variety of additional spy planes, particularly the Mach 3 SR-71, in the decades after the United States mastered the art of conducting reconnaissance from space—even after the quality of satellite photos equaled or surpassed that of the lower flying aircraft. U-2s and/or SR-71s were used to photograph installations, military facilities, and military developments in

Cuba, Nicaragua, Libya, and Bosnia. The U-2 has also been used to monitor compliance with cease-fire agreements such as the 1973 agreement between Israel and Egypt and the 1991 agreement between Iraq and coalition forces.

Other nations employed their own reconnaissance aircraft—usually modified fighters or bombers. France has used specially configured Mirage fighters, equipped with a variety of sensors, whereas Britain has relied on modified Canberra bombers, which were employed during the 1982 war over the Falklands.

Another type of overhead imagery system has some of the virtues of satellites and aircraft, and some of its own advantages. Unmanned aerial vehicles (UAVs) equipped with electro-optical systems or infrared sensors are operated without a pilot by remote control—thus the political risks and risk to life involved in manned reconnaissance operations are eliminated. Like aircraft they can move in a straight line—following troops, refugees, or a group of mobile missiles in transit. Unlike satellites or aircraft, UAVs can remain over a target, at high altitudes, for extended periods of time (e.g., twenty hours), keeping watch on a particular target or area, such as a terrorist training camp or nuclear test site.

Whereas the United States began operating *drones* (pilotless aircraft that could not be maneuvered) and UAVs during the Cold War, it is in the post–Cold War that UAVs have become a more significant component of U.S. reconnaissance activities. The CIA began flying Predator UAVs over Bosnia in 1994. After the initiation of military operations in Afghanistan the United States began equipping Predators with Hellfire missiles so that immediate action could be taken if imagery indicated the presence of a terrorist target. Even more recently, the United States has been deploying the Global Hawk UAV—capable of operating at over 60,000 feet for twenty hours and carrying electro-optical, infrared, or radar imaging sensors.

BENEFITS AND LIMITATIONS

That imagery collection can produce intelligence of enormous value has been demonstrated throughout the 20th century. During World War I photographic reconnaissance provided intelligence on enemy troop movements. In World War II all sides conducted extensive photographic reconnaissance operations to identify targets and assess the impact of bombing runs—particularly important in an era in which precision bombing was only a dream.

During the Cold War satellite imagery (along with monitoring of the telemetry from Soviet missile tests) was of primary importance for the United States in assessing the capabilities of Soviet strategic forces. Imagery was vital in determining the numbers of intercontinental ballistic missiles (ICBMs) and submarine-launched ballistic missiles and the locations of ICBM fields. Today it permits monitoring (albeit not perfect monitoring) of Iranian and North Korean nuclear activities, Chinese intermediate missile deployments in regions near Taiwan, and the construction of terrorist training camps.

Soviet photographic reconnaissance satellites allowed the Kremlin's rulers to be confident that they had a good understanding of U.S. strategic capabilities. Collectively, the existence of overhead reconnaissance and other technical collection capabilities allowed the negotiation of arms control agreements—particularly the Strategic Arms Limitation Treaty (SALT) and the Strategic Arms Reduction Treaty (START)—because each side had an independent means of monitoring compliance, and provided reassurance that the other side was not in the process of preparing for a surprise attack.

Today the international environment is significantly different from what it was two decades ago—with the collapse of the Soviet Union, the concern over rogue state acquisition of nuclear weapons, the threat from fundamentalist Islamic forces, and the global reach of international terrorist organizations such as Al Qaeda.

Despite those developments, imagery capabilities remain a significant factor in the ability to gather intelligence. Imagery can still identify the dispersal of strategic and conventional military forces, from missile silos to airbases, the presence of above-ground nuclear facilities, and suspicious construction activities. It remains important to treaty verification, and it can provide warning of events that a nation's senior officials and diplomats would seek to forestall with advance knowledge—as when, in 1995, the United States was able to persuade India to forgo conducting a planned nuclear test after imagery indicated that preparations were under way.

It also remains vital in providing support to military planners and combat commanders when diplomacy fails. Imagery continues to help identify potential targets as well as particular points in such targets to attack, and to assess the damage done from such attacks. And with real-time capabilities, properly equipped commanders in the field have the ability to look over the horizon and see the enemy—his numbers, deployments, and movements—without delay.

Of course, the fact that imagery collection systems can produce significant intelligence does not necessarily imply that they are not without their limitations or that they are, in relative terms, as valuable as they were in an earlier era. Thus, key documents that may shed light on diplomatic or military intentions or capabilities cannot be photographed remotely. At times, such documents can be obtained via a human source.

Imagery systems can be subject to denial and deception. A nation that knows or suspects that some activity—for example, preparations for a nuclear test or WMD production—would be of interest to another nation's reconnaissance satellites may take care to eliminate or minimize the chance that those satellites will detect the preparations. Denial measures that might be taken include operating at night, not operating when a foreign reconnaissance satellite is estimated to be in range, and conducting test preparations under cover of another, more innocuous activity. A significant factor in India's ability to surprise the United States with its 1998 nuclear test was the precautions taken to avoid detection by U.S. spy satellites—including operating at night.

Deception involves more than preventing a foreign satellite or aircraft from obtaining an image of a target. It involves actively trying to induce another nation's imagery interpreters to draw false conclusions. Dummy military equipment, such as fake aircraft, can be deployed at an airbase to produce erroneous conclusions concerning the number and location of aircraft. Or a building might be made to appear as if it had been damaged by fire—as Libya unsuccessfully attempted to do with a chemical weapons facility. Alternatively, a nation may cover up signs of a certain activity to create the impression that no activity is under way. Thus, not only did India hide its preparations for a nuclear test in 1998, it made sure that when U.S. satellites were overhead they saw the same reassuring scene every time—including the same vehicles parked in the same spaces they would be in when no preparations were under way.

The inability of imaging sensors to penetrate through buildings provides a natural protection for targets. Assessing what is going on inside a building may depend on combining the hard data images with assumptions, and even speculation. Thus, in 1979 a U.S. satellite photographed the Severmorsk Weapons Storage Facility. The imagery allowed U.S. interpreters to identify a new arched roof bunker, a weapons-handling and maintenance facility, storage and support facilities, and a weapons assembly facility. But determining exactly what was inside the facility was more difficult. A Defense Intelligence Agency document noted that:

> this bunker, now almost completed, measures approximately 45 meters × 12 meters and will *probably* be used to store SS-N-14 missiles. A second, similar bunker is in the early stages of construction. . . . Taking into account the measurements of the almost completed bunker and *assuming* only one-level stacking with a central aisle for maneuvering will be utilized, about 60 SS-N-14 missiles may be stored. Further, *assuming* the second bunker to be constructed will be the same size, a similar number of stored missiles would bring the total capacity to 120.[11] [Emphasis added.]

A far more recent example of the limits of imagery is the faulty intelligence associated with the 2003 invasion of Iraq. UN inspectors left Iraq in December 1998 after Saddam Hussein's regime policy of obstruction made it impossible for them to carry out their mission. Over the next five years U.S. reconnaissance satellites produced images of reconstruction activities at sites that had been associated with each component of Iraq's weapons of mass destruction program—a nuclear weapons-related site at Al Furat, a chemical weapons site at Fallujah, a biological weapons facility at Abu Ghurayb, and a missile facility at Al Mamoun.[12] Satellite imagery also revealed the presence of vehicles around the facilities and the movement of vehicles to and from the facilities. But the imagery itself did not provide conclusive evidence of what was going on inside those facilities. Thus, interpreters were forced to draw conclusions based not only on the images in front of them, but on assumptions based on past Iraqi activities—assumptions that turned out to be incorrect.

Thus, imagery, like all other forms of intelligence collection, can produce significant intelligence in support of a nation's diplomatic or military endeavors. But there may also be situations when the information it produces is not truly conclusive and one must obtain additional ("collateral") data from another source—sometimes communications intercepts, sometimes a spy—to reach the correct conclusions.

NOTES

1. William E. Burrows, *Deep Black: Space Espionage and National Security* (New York: Random House, 1986), p. 28.

2. Ibid., p. 32.

3. Jeffrey T. Richelson, *A Century of Spies: Intelligence in the Twentieth Century* (New York: Oxford University Press, 1995), pp. 33, 96–100, 157–72.

4. Jeffrey T. Richelson, *The U.S. Intelligence Community* (Boulder, CO: Westview, 1999), pp. 153–54

5. Ibid., p. 155.

6. On developments with respect to reconnaissance satellite proliferation see, Jeffrey T. Richelson, "The Whole World Is Watching," *Bulletin of Atomic Scientists* (January–February 2006), pp. 26–35.

7. Office of Research and Reports, CIA, *Visual-Talent Coverage of the U.S.S.R. in Relation to Soviet ICBM Deployment, January 1959–June 1960,* July 11, 1960, pp. 101–13, in *CORONA: America's First Satellite Program,* ed. Kevin Ruffner (Washington, DC: Central Intelligence Agency, 1995).

8. Norman Polmar, *Spyplane: The U-2 History Declassified* (Osceola, WI: MBI, 2001), p. 208.

9. J. Michael Selander, "Image Coverage Models for Declassified Corona, Argon, and Lanyard Satellite Photography: A Technical Explanation," in *CORONA: Between the Sun and the Earth,* ed. Robert A. McDonald (Baltimore: ASPRS, 1997), p. 177; Photographic Interpretation Center, Central Intelligence Agency, *Joint Mission Coverage Index, Mission 9009, 18 August 1960,* September 1960, pp. 115–25 in Ruffner, ed., *CORONA*.

10. On the history of the U-2, see: Chris Pocock, *The U-2 Spyplane: Toward the Unknown* (Atglen, PA: Schiffer Military History, 2000).

11. *Documents From the Espionage Den (52): U.S.S.R.: The Aggressive East, Section 3-2* (Teheran: Muslim Students Following the Line of the Imam, n.d.), pp. 40–41.

12. National Security Archive Electronic Briefing Book No. 88, *Eyes on Saddam*, April 30, 2002, available at http://www.nsarchive.org.

5

THE IMPORTANCE AND FUTURE OF ESPIONAGE

FREDERICK P. HITZ

WHEN PRESIDENT TRUMAN SIGNED THE NATIONAL SECURITY ACT of 1947 into law, creating the Central Intelligence Agency (CIA), he believed not that he was creating a new espionage organization for the United States, but rather that he was greatly improving the manner in which important national intelligence would find its way to his desk. Earlier he had disestablished the Office of Strategic Services (OSS), the wartime foreign intelligence collection and analytical entity, declaring that he did not want an American Gestapo in peacetime. By 1947, he had changed his mind on the need for a civilian intelligence organization for three principal reasons. First, and most important, the lessons of the 1941 Pearl Harbor attack strongly suggested the need for greater early warning of a future surprise attack on the United States. Second, he needed a centralizing intelligence organization that would gather and analyze all the intelligence reports headed for the Oval Office and attempt to make something coherent out of them so he would not have to do it himself. It is not clear that he wanted the new organization to go out and collect intelligence information on its own, as this had been tasked primarily to the Armed Services and to the Federal Bureau of Investigation (FBI). Third, he was convinced by Secretary of the Navy James Forrestal and others in his Cabinet that the U.S.S.R. would become a problem now that the Nazis were defeated, and that he needed a window into Stalin's thinking and imperial ambitions, especially in Western Europe. The Cold War was beginning.

The CIA got off to a slow start. Its early directors were military men who had a limited idea of the coordinating role the CIA was intended to play and were aware of the bureaucratic sharks circling them, representing the parochial interests of the military departments, the FBI, and the State Department, all of which wanted to maintain their direct access to the president on intelligence matters.

Two events conspired to change this modest approach. George F. Kennan penned his famous "Long Telegram" from Moscow, alerting Washington in 1946 to Stalin's imperialist designs on that part of Europe not already under Soviet control, and recommending a policy of "containment" by the United States. At the very least, this would require affirmative action by the United States in funding democratic political parties, labor unions, student groups, and cultural organizations in Italy, France, and Western Germany to oppose the Communist elements seeking to dominate these entities. In addition, to be most effective, the hand of the United States should remain hidden. The military were not the appropriate weapon to oppose clandestine Soviet infiltration and the State Department rejected the assignment, so the fledgling CIA got the job. Luckily, there was language in the 1947 Act creating the CIA that directed it to perform, with the authorization of the president, vice-president, and secretaries of defense and state acting as the National Security Council, "such other functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct." Thus was created the covert action responsibility of the CIA that grew enormously from 1948 to 1952 under the leadership of Frank Wisner. Wisner's so-called Office of Policy Coordination (OPC) was lodged ostensibly in the Department of State, but in reality it was an operational element of the CIA.

The second major development was the arrival on the scene of two savvy Directors of Central Intelligence (DCI). Air Force Lieutenant General Hoyt S. Vandenberg and retired Army General Walter Bedell Smith (who had been Eisenhower's wartime chief of staff) knew what the organization required to move up to the big leagues and were prepared to fight for it. Vandenberg was responsible for securing for future DCIs the requisites to do their job. The National Security Acts of 1947 and 1949 that he had lobbied for (and that had also shown the handiwork of an outside commission appointed by President Truman in 1949 that included Allen Dulles) gave the DCI unparalleled authority in Washington. They gave Vandenberg and his successors as DCI the power to: hire and fire his subordinates; spend money on their own say-so without further justification; short-circuit the federal government's cumbersome procurement authorities in order to perform the intelligence mission; and act across the range of intelligence collection, analysis, and dissemination responsibilities. The scope of authority was to include activities from classic espionage, to special operations (covert action), to all-source analysis, to briefing the president's National Security Council. In short, Vandenberg got the CIA, and the DCI especially, off to a running start before he returned to the Air Force. Bedell Smith took the new organization the rest of the way.

Bedell resuscitated the CIA's estimative intelligence, a function that had earned its stripes during the wartime OSS period but had lain dormant upon the OSS's demise. Estimative intelligence looks out to the future, attempting to foresee problems of concern to the president that may be coming down the line. With Truman's go-ahead, Bedell created a Board of National Estimate reporting to the

DCI, led by the same Harvard history professor, William Langer, who had put it together for General Donovan during World War II. Professor Langer managed to convince a number of wise men from the nation's best universities to work for him and Bedell, tasking them with tracking the future course of the Cold War rivalry with the U.S.S.R.

DCI Smith also made it clear that covert action and special operations existed in a chain of command extending from the DCI, and in coordination with the other espionage capability that the DCI oversaw for the president, the Office of Special Operations (OSO). He thus contrived to bring Wisner's OPC into the CIA in fact.

The OSO's responsibility was to gather foreign intelligence information by secret means (i.e., classic espionage). It was often stumbling over or wandering into operations conducted by the OPC, because the foreign actors who stole the secrets were often the same ones who could manage the propaganda or organize the political meetings for the OPC. This is an important historical point. If the CIA did not take the field to secretly oppose Soviet propaganda, backdoor electioneering, and subversion in Western Europe, several of the United States' most important allies might have been in jeopardy. Furthermore, intelligence activity that connoted "action" was very much in the American character. It drew many adherents in the early CIA both because there was a perceived need (as the constant stream of national security directives from the president and National Security Council attested) and because, if successful, you could see the results. At the same time, the slow, painstaking process of recruiting spies to report on happenings behind the Iron Curtain and in the Soviet Union itself had to be undertaken. In the late 1940s and 1950s this was difficult and dangerous work, new to Americans of whom very few spoke the relevant languages, Russian, Polish, Czech, and Hungarian. It required a patience and professionalism in terms of tradecraft that the OPCers sometimes overlooked or made fun of. The spy recruiters and handlers (of whom DCI-to-be Richard Helms was a prominent representative) were dubbed "the prudent professionals" and were not as esteemed or promoted as quickly as the OPC "action" types. Bedell tried to end all that by making of the OSO and OPC one clandestine service, directed by one chief, Allen Dulles, who reported to him. Over time it worked. The two skill sets became a little more interchangeable, although DCI Smith noted in his farewell remarks to President Truman that he thought the CIA was expending far too little effort with too meager results in acquiring intelligence penetrations of the Soviet Union.

Bedell was, of course, succeeded by DCI Allen Dulles, who jumped on the Eisenhower administration's desire to contain the Soviet Union by mounting covert action programs rather than confronting it with U.S. military force. As Supreme Commander, Allied Forces, Europe, in World War II, General Eisenhower had been a consumer of Britain's ENIGMA German code-breaking successes and knew both the role and the limitations of intelligence. As president, he believed strongly that the Soviet worldwide advance had to be stopped, if not rolled back,

and covert action operations seemed a cheap and relatively low-risk way to do it. Enamored of early successes in overthrowing regimes in Iran (1953) and Guatemala (1954), the president and his advisors at the CIA grew accustomed to pushing the envelope in operations, overlooking close shaves and longer term backlash.

However, this extraordinary progress in spying on the U.S.S.R. and containing its influence during the Eisenhower years encountered several highly public setbacks as well. The revelation in May 1960, initially denied by President Eisenhower, that the Soviets had shot down a U-2 surveillance aircraft flying over Soviet territory, disrupted the Paris summit. The plan to secretly train Cuban exiles to land on Cuban soil to overthrow the Castro regime—later adopted by President Kennedy, and put into practice half-heartedly in an indefensible location at the Bay of Pigs—abruptly ended a run of successes by the CIA. Kennan's X article had alerted Washington to the bitter adversities ahead in confronting as politically hardened a foe as the Soviets; so it was naturally only a matter of time before a handful of poorly conceived or blighted operations gave the CIA an enduring notoriety and taint abroad, and dispelled the aura of the Agency's infallibility around Washington. The Bay of Pigs disaster triggered the replacement of Allen Dulles by John McCone, whose signal innovation as DCI was to put the analytical consensus within his own Agency under intense personal scrutiny.

The tattered doctrine of plausible deniability, however, still held an occasionally disproportionate allure for Kennedy and later presidents. After a national wake-up on the shores of Cuba's Bay of Pigs, JFK raised CIA's operational arm from the ashes, only to shoot for the moon all over again in *Operation Mongoose*, which saw the Agency embark on a rash of sometimes frantic missions to overthrow a now-entrenched Fidel Castro.

Despite the evident hazards of the profession, presidents relied substantially on CIA spies in Berlin to counter Soviet pressure there. The Eisenhower-Kennedy years were the beginning of the era of America's greatest technical intelligence successes as well, with spies and electronics working hand-in-glove in Berlin and elsewhere; with the construction of the U-2 high-altitude photo-reconnaissance aircraft; and with the refinement beginning in the 1960s of overhead satellite surveillance, eventually able to communicate images and intercepted electronic signals to Washington in real time. Nonetheless, it was on Cuba, in the October missile crisis in 1962, that U.S. intelligence showed that it had arrived at a position of sufficient maturity in its collection systems to be able to support President Kennedy with intelligence from all three principal collection branches: SIGINT, IMINT, and HUMINT. The U-2 flyovers were the first to supply photographs of Soviet medium- and intermediate-range ballistic missiles being transported to, unloaded, and installed in Cuba. Signals intercepts pointed to a heavy buzz of communications around the part of the island where the missiles were being installed, and human sources witnessed the transfer of mysterious long tubes on highways too small to accommodate them. Although there were many details that human sources were unable to provide, our principal spy,

Oleg Penkovsky, from his vantage point at the pinnacle of Soviet military intelligence, reported on the ranges and characteristics of the IRBMs and MRBMs which were being installed. He also revealed that General Secretary Khrushchev was way out in front of his Politburo in thus challenging the United States so close to its home territory.

The fact that President Kennedy had Penkovsky's insights into Khrushchev's overexposure, confirming the observations of his own former ambassador to the U.S.S.R. Llewelyn Thompson meant that JFK was prepared to give up the strategic advantage of a surprise attack on the installation and, in a masterstroke of statecraft, give General Secretary Khrushchev an opportunity to escape from the corner into which he had painted himself. In my view, this was the apex of U.S. intelligence support to the president during the Cold War.

After October 1962 prosecution of the Vietnam War became the overriding national security concern of Presidents Kennedy, Johnson, and Nixon. The CIA built up its presence in South Vietnam and collected useful human intelligence, from captured Vietcong and North Vietnamese prisoners especially, that permitted it to report consistently that the Government of South Vietnam (GOSVN) was unlikely to prevail in the war unless it took a more active role in the fighting and was able to win over greater support in the Vietnamese countryside. The CIA's rejection of the validity of high body counts that were held by American military intelligence to signal attrition in the North Vietnamese capacity to wage the war is reminiscent of today's intelligence controversy about the import of the nonexistence of weapons of mass destruction (WMD) in Iraq.

In the case of Vietnam, the CIA more or less stuck to its guns that North Vietnam was not being defeated in 1968 despite its loss of manpower, whereas it was "dead wrong" in its assessment of the existence of chemical and biological weapons stores in Iraq in 2003, according to the Silberman-Robb Presidential Commission Report. In both cases the requirement of good, on-the-ground, contemporaneous human source reporting was critical to CIA intelligence judgments. In Vietnam we had it, whereas in Iraq we did not. Silberman-Robb found that the critical National Intelligence Estimate of October 2002 on Iraqi WMD was based on unilateral spy reporting that dated from 1991, and UN weapons inspection reporting that dated to 1998. There was no direct, on-the-ground HUMINT after that before the outbreak of the war. Over the decades, the NIE process had taken on its share of taxing intelligence puzzles, but it was clearly compromised and out of date in this one.

It is ironic that, as today, the great blows to the quality and competence of CIA human source reporting in the 1970s were delivered during a Republican presidency, on the watch of a national security establishment that valued and to some extent depended on good intelligence for its activist foreign and defense policy. Although Richard Nixon privately disparaged the Ivy Leaguers at Langley whom he believed had favored his opponent in the 1960 presidential race against JFK, he needed good intelligence on Vietnam to support the Paris peace talks Secretary of State Henry Kissinger was conducting with the North Vietnamese,

and also his overtures to China. Indeed, when it looked as if an unabashed Marxist, Salvador Allende, was poised to win the Chilean presidential election of 1970, it was to the CIA that President Nixon turned, improperly bypassing the rest of his foreign policy establishment and the U.S. Congress to mount a coup against a democratically elected Latin American leader.

Watergate and the Nixon resignation turned the tide against this manifestation of executive imperialism, while the CIA caught a fair measure of popular and congressional backlash. Investigative reporter Seymour Hersh wrote a series of articles in the *New York Times* in December 1974 setting forth the ways in which the CIA (and the FBI) had illegally spied on American anti–Vietnam War protesters, opened people's mail, tested hallucinogenic substances on unwitting subjects, and otherwise acted outside the bounds of an already broadly demarcated charter without the knowledge of Congress or the American people.[1]

Congressional reaction was swift and severe. The U.S. Senate and House of Representatives each convened investigating committees to hold extensive public hearings on CIA abuses. Senator Frank Church, a Democrat from Idaho who was running for president, tried to lock then-DCI William Colby into admissions that the Agency had attempted to assassinate several world leaders such as Fidel Castro, Patrice Lumumba of the Congo, Rafael Trujillo of the Dominican Republic, and Salvador Allende, without a president's authorization, claiming that the CIA was a "Rogue Elephant." In the end, the Church Committee was unable to substantiate these allegations. There was some assassination plotting at the CIA, directed by presidents, but none was shown to have been carried out successfully.

However, the Senate's inquiry caused President Ford to create a blue ribbon panel headed by Vice-President Rockefeller to look into the matter and to preempt Congress's certain desire to legislate restrictions on U.S. intelligence activity. Thus was born the effort to establish greater executive and legislative branch oversight of the intelligence community. President Ford promulgated Executive Order 11905 in February 1976, which banned assassination of foreign political leaders by U.S. intelligence operatives or their surrogates, among other restrictions. The order contained a number of additional dos and don'ts that were binding on the intelligence community, and it was reissued by Ford's successors, Carter and Reagan, in substantially the same form. After several years of trying to pass legislation establishing more comprehensive and binding charters for intelligence community agencies such as the FBI, CIA, NSA, and NRO, real-world dangers posed to the United States by the Soviet Union caused the public and Congress to regain some equilibrium on the subject of further restraining U.S. intelligence gathering capabilities, and the effort was dropped. Congress settled for one paragraph in the Intelligence Authorization Act of 1980. It required the DCI and the president to keep Congress "fully and currently informed" of all intelligence activities, including covert action, consistent with the president's constitutional authorities and the DCI's duty to protect "sources and methods from unauthorized disclosure."

Congress believed it could settle for this paragraph instead of the several-hundred-page charter bill, because it had established in 1975 and 1976 permanent oversight committees of the House and Senate to review intelligence community programs and operations, just as every other department and agency in the executive branch is reviewed.

Some argue that since the creation of the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI), with rotating memberships after seven years service, the CIA has never been the same aggressive collector of human intelligence that it was during the height of the Cold War. I disagree. The world had changed by 1975. Although the Soviets still maintained a nuclear arsenal pointed at America's heartland, it was on the downhill side of the slope economically and politically. It had an aging leadership and an increasing inability to provide for the needs and wants of its people. The United States was receiving more volunteers as spies from the Soviet Union, as its high-ranking cadres became increasingly gloomy about the country's future prospects. In the United States Vietnam had exploded the postwar consensus surrounding U.S. foreign policy, and a stronger demand for oversight and accountability for all of America's overseas activities had emerged.

When this era of intelligence reform ended, the full-time housecleaners who worked at Langley and the FBI had managed to stay out of the headlines for the most part. Spying against private citizens clearly violated the 1947 Act but made for no more than a sideshow when compared to spy-hunting inside the U.S. government. Light almost never shines on this most sensitive area of surveillance, counterespionage, but in this domain of intelligence work especially, tumult has been virtually inseparable from tradecraft. Penetrations and double-crosses can be expected in the competition among major intelligence services, but the integrity of intelligence operations rests on how well very fragmentary and circumstantial clues about possible security breaches can be read. Moles were often uncovered only years after their work got started. Indeed, when the Cold War did end abruptly, counterespionage work was not ready to wind down but was putting itself in high gear, as Americans were making inroads into the former Warsaw Pact services, shedding light on turncoats here at home.

American intelligence contended with a number of notorious penetrations in the Cold War, and most spectacular of these was the early discovery that the Soviets had recruited the top British liaison official in America, Kim Philby. Philby had until then been regarded as one of MI6's best men—a man in line to be its next director, a brilliant and affable character, and a mentor to many of Langley's rising stars. The United States had depended heavily on him personally for many of our early postwar efforts in Europe. Philby had been in a position to alert Moscow to many of the biggest and most sensitive intelligence exploits under way: the development of the atomic bomb and the VENONA project, through which the NSA was attempting to break encrypted communications from the Soviet embassy and the New York consulate during World War II. But he could

not prevent the NSA from discovering an old code-name, Homer, referring to a British mole in the U.K. embassy in Washington. Homer was one member of the entire Cambridge Five spy ring, another of whom was quickly tied to Philby, as a friend boarding at Philby's home. In 1951, Philby's official career effectively ended. But it took another decade's worth of revelations for his career as a double-agent to be sufficiently understood to put him in criminal jeopardy, whereupon he defected.

James Jesus Angleton, the CIA's master spy-hunter, was one among many of Philby's former friends on whom his treachery left a lasting impression. Angleton's occupation at the CIA was actually not widely known. He was simply, "the Ghost of Langley," the man who showed up unannounced at the DCI's office for an immediate, private audience with the boss. A classics major and poet at Yale who moved in the same circles as T.S. Eliot and Ezra Pound, Angleton was picked toward the beginning of his career to run the counterintelligence operation in Rome, during the crucial 1947 elections that kept the Italian Communist Party out of power. Angleton's early career also solidified CIA liaison operations with other services, including those of Britain and Israel. And he worked alongside the Mafia during his Rome posting. The Mafia had operated on behalf of the OSS in wartime Italy, and had helped to perfect some of the more lethal aspects of the CIA's tradecraft.

Angleton's cunning instincts came to the attention of Allen Dulles, who asked him in 1954 to head the CIA's counterspy operations. By 1959, Angleton had unearthed Jack Dunlap as a mole in the NSA who had reached high-level "no inspection" clearances. But in retrospect, though the Philby affair had ignited Angleton's imagination, it had not furnished the CIA with the kind of tradecraft lessons that would shed a much clearer light on future penetration controversies. In 1961 Angleton seemed to be nearing more breakthroughs, having been given personal charge of debriefing a defecting KGB major, Yuri Golitsyn, but Golitsyn became increasing problematic for the CIA over time. In addition to the key information he did betray, he was willing to speculate endlessly about other penetrations of U.S. intelligence, and spun out theories that Angleton showed himself ready to embrace. Among the most troubling questions he raised was the identity of the mole Sasha, a code-name that sparked the most tortuous inquisition that the Agency would ever launch: These investigations had such disproportionate impact on work at the Agency that their records remain completely restricted to this day. And Golitsyn insisted with some vehemence to CIA officers, after each subsequent defector surfaced, that anyone to follow him would almost certainly be a plant, blunting the CIA Counterintelligence Staff's instincts. The name of one of those subsequent defectors, Yuri Nosenko, was much later cleared of being a Soviet double agent, but Nosenko fell afoul of his own glaring penchant for fabrication, and at first cast the most severe suspicions upon himself. Working on Angleton's behalf, J. Edgar Hoover's FBI went to extremes to try to extract a confession from Nosenko but were ultimately unsuccessful. Meanwhile, Nosenko had languished in solitary confinement for three years. In the aftermath,

Hoover judged Angleton poisonously misguided, and the debacle helped to drive a permanent wedge between the FBI and CIA, from which neither agency extricated itself until after September 11.

Angleton put at least fifty intelligence officers under surveillance during his career, and removed at least sixteen from the service. Problems at the CIA became more severe as his views darkened into clinical paranoia over the course of the 1960s. The only personal trust Angleton was ultimately able to sustain was in his closest circle. Meanwhile he elaborated plots with Golitsyn's help. As facts became hunches, and his hunches increasingly bordered on the absurd, he came into permanent conflict with the Agency's leadership. Finally, he could not find a distinction between political loyalty and personal allegiance to his theories. He was barred from direct contact with Golitsyn in 1968 by DCI Dick Helms, and ushered into retirement in 1974 by DCI Bill Colby, while the Hersh revelations of domestic spying were in the headlines. His Counterintelligence Staff was diminished from 300 to 80.

The counterespionage underworld that defends against other powerful foreign intelligence agencies is a reality in which things remain extraordinarily indeterminate. A myriad of conceivable avenues might lead to operational betrayal. Angleton's version of reality was to adopt the premise that the most successful Soviet campaigns were those of knowingly false information—disinformation—that could operate at a great remove from the Agency's headquarters. Penetrations were less important than the false tracks onto which the CIA could be lured. But in truth the kinds of judgment calls are immensely difficult that spy-hunters must make to arrive at breakthroughs in cases of penetration. Major revelations might never come down the road. And surveillance might fail to turn up any mole at all. Moreover, in the life-or-death stakes of the Cold War, there was always the potential that too broad or intrusive a mole-hunt would leave more self-inflicted damage to CIA operations than unearthing a mole would stanch. Nevertheless, crucial countermeasures still had to be taken, and in counterespionage it was often the effort to run down trails of minor lifestyle and procedural misconduct that kept operations secure.

Philby was the result of a relatively spectacular breakthrough, but the Aldrich Ames and Robert Hanssen penetrations during the 1980s and 1990s remained almost entirely invisible for years after the investigations got rolling. Ames and Hanssen did their damage over a period of time when CIA attitudes about lifestyle and procedural misconduct had remained too lax for too long. The Agency lost the distinction between operations in the outside world and the life of discipline required inside. Most espionage operations are carried out in the gray areas of administrative procedure; but over the years, these moles built microcosms of that mission right in the offices that they ran at the CIA and FBI. Like all other skilled professions, intelligence officers have to accept a high level of personal autonomy in those they rely upon; but the basics of tradecraft, on-time reporting, and drug and alcohol-free behavior are important too. Over the long haul, the maintenance of strict operational routine and personal integrity goes a

fair ways toward assuring the success of the intelligence community in its operational mission.

Within the CIA, the chaos that followed Operation CHAOS (the controversial CIA domestic mail-opening program revealed in 1974) lasted well into the Carter presidency and the tenure of DCI Stansfield Turner. President Carter put the CIA back on the offensive in his changing attitude to the Sandinistas in Nicaragua, and the covert action he instigated to oppose the Soviet takeover of Afghanistan in 1979. Still, it remained for Ronald Reagan to initiate an across-the-board revitalization of both U.S. defense and intelligence resources that would reverse the post–Vietnam War drawdown and counter ongoing outbreaks of Soviet aggression. President Reagan authorized a covert action to train and reinforce the *contra* resistance to the Marxist Sandinista revolution of 1979 in Nicaragua, and a second covert program to build up the *mujahedeen* factions opposing the Soviet-controlled government in Afghanistan. At the same time, he initiated a research program to intercept incoming missiles in space. The Kremlin began to believe the United States was trying for a first-strike capability against the U.S.S.R. and initiated a worldwide intelligence alert called Project Ryan to report on indicators confirming such an effort. At the same time, old age and sickness were removing Soviet premiers at a record rate. In March 1985 a completely new figure ascended to power in the Kremlin, Mikhail Gorbachev, who was focused on curtailing Soviet commitments to defend communism everywhere (the Brezhnev Doctrine) and reforming the economy to provide a better response to the needs of the Soviet people. Meanwhile the Reagan administration was having a difficult time keeping the U.S. Congress on board for the operation to support the *contra*s. After the second amendment curtailing CIA support for the *contras* passed Congress—and was signed into law by the president because it was attached to an omnibus year-end appropriations bill—some members of the administration on the National Security staff and in the CIA concocted a scheme to sell embargoed weaponry to Iran in exchange for information about terrorists who had abducted Americans in the Middle East, using the proceeds from the sales to supply weapons illegally to the *contras*. The Iran-Contra scheme finally blew up in the press in fall 1986, sending the Reagan White House and William Casey's CIA into a tailspin.

It took the appointment in 1987 of Judge William Webster as DCI, a former Director of the FBI and U.S. Court of Appeals judge, to restore legitimacy and integrity to CIA operations after the Iran-*contra* fiasco. Meanwhile, CIA covert operators got congressional approval to supply Stinger missiles to the Afghan *mujahedeen*, a policy that proved pivotal to driving the Soviets out of Afghanistan. As unintentionally transparent as the Nicaraguan covert action was to the world, so the cooperation by the CIA with the Pakistani intelligence service to supply armaments to Afghani and Arab guerillas in Afghanistan was painted as a state secret within the boundaries of "plausible deniability." The Soviets knew where the weaponry, especially the Stingers, was coming from, but they were in

no position to do much about it, despite the concerns of Pakistan's nervous chief of state, Mohammed Zia-ul-Haq.

To date, the Afghan covert action has been the last big successful clandestine political operation mounted by the CIA in which the U.S. hand did not show to an impermissible degree. By and large, the CIA officers involved kept their promise to Pakistan's rulers that they would physically stay out of Afghanistan and work through the Pakistani intelligence service, the ISI. The advent of both round-the-clock cable news programming and instant worldwide communications via the Internet have successfully impinged upon the United States's ability to maintain the necessary secrecy of a major covert political operation. This was made manifest in the administration of President George H.W. Bush, when the president, despite his tour of duty as DCI and his appreciation for the role of intelligence, turned instead to the American military to deal with both Manuel Noriega in Panama in 1989 and Saddam Hussein in the first Gulf War in 1991. When President Clinton sought to make use of covert action in overthrowing Saddam in the mid-1990s, he found it was impossible. Congress had gained an appetite for micromanaging an operation that could have high domestic stakes, and the CIA had too few covert assets to bring it off.

By the same token, viewed in retrospect, in the mid-1980s it would turn out that the United States had suffered unprecedented high-level penetrations of its intelligence services, through the handiwork of Aldrich Ames in the CIA and Robert Hanssen in the FBI. Ames began his espionage for Soviet handlers in March 1985 in order to get $50,000 to buy himself out of debt. He was a thirty-year spy in the CIA's operations directorate who had specialized in Soviet matters, arriving at a senior level even though he had a mediocre record—which included numerous episodes of alcohol abuse, security violations, and a chronic inability to get his financial accountings and contact reports about meetings with Soviet officials in on time. In short, Ames probably should never have been permitted to be on the front line, meeting and assessing Soviet officials one-on-one. But he was. And he used his position and his knowledge of how both the Soviet and U.S. intelligence systems operated to betray, over a period of nine years, every agent working for the United States against the U.S.S.R.; details of numerous U.S. operations against the Soviets; and the names of his colleagues who were engaged in the effort. Ames's betrayal led to the certain execution of ten U.S. spies and probably more, along with the compromise of hundreds of U.S. intelligence operations. The arrest of Aldrich Ames in 1994 provoked a wave of disillusionment and dismay in the American public, and among the congressional oversight committees, that such a sloppy and seemingly inept spy could betray so much over such a long period, not only without being caught, but without the CIA having mounted a serious effort to track him. The damage to the Agency's reputation was nothing short of devastating.

For the FBI, no less damaging was the tale of Robert Hanssen, a dour misfit who had used his superior information technology skills to eventually burrow into the deepest corners of the Bureau's counterintelligence operations against

the U.S.S.R. Hanssen managed to turn over vast amounts of operational detail and names of U.S. agents to the Soviets in an on again–off again career of espionage that began in the late 1970s and continued until his arrest in February 2001. Hanssen's case was a tougher one to crack than Ames's because Hanssen had been careful never to meet with his Soviet handler, conducting all his business with the Soviets through dead drops in a park near his home in Northern Virginia. Furthermore, Hanssen had compromised many of the same spies named by Ames or by Edward Lee Howard, another CIA turncoat of the period; so it took an analysis of operations that had gone sour that could not have been compromised by Ames or Howard, and also the help of a Soviet source, before Hanssen's own activities could be distinguished and an arrest finally made.

At the same time that these spy wars were taking place between the Soviet and U.S. intelligence services, the CIA was beginning to enjoy real success in running Soviet and Bloc volunteer spies who were supplying vast amounts of useful intelligence information about Soviet and Warsaw Pact war-fighting plans in Europe, and Soviet military research and development (R&D). In the former case, Ryszard Kuklinski, a high-ranking member of the Polish General Staff, passed the CIA all of the Warsaw Pact plans that crossed his desk from 1972 until his defection in 1981; and in the second case, Adolph Tolkachev provided his U.S. case officer with the latest Soviet military R&D on stealth technology and air defense missilery from the late 1970s until 1985, saving the U.S. taxpayer millions of dollars in unnecessary defense expenditure. These successful Soviet spy volunteer recruitments at the end of the Cold War, and others like them, proved the value of a vigorous human source collection program at the time that the Soviet regime was under severe internal stress.

The need for espionage did not disappear with the dismantling of the Berlin Wall in 1989 and the dismemberment of the U.S.S.R. in 1991. The successor Russian government kept its intelligence officers in the field and the West at bay on a number of important issues. Yet, over time, the threats targeted by American intelligence agencies began to shift. As authoritarian regimes calcified or collapsed over the decade of the 1990s—frequently ex–Cold War client governments—the new threats would become proliferating weapons of mass destruction and emerging nonstate terrorist factions, exemplified by Osama bin Laden and Al Qaeda.

In a series of bold and ever more sophisticated attacks, beginning with that on the Khobar Towers, a U.S Air Force billet in Saudi Arabia in 1997; followed by the bombings of U.S. embassies in Dar es Salaam and Nairobi in 1998; and the attack on the *U.S.S. Cole* in 2000, this affluent Saudi veteran of the *mujahedeen* effort against the Soviets in Afghanistan, Osama bin Laden, showed he was capable and desirous of inflicting unacceptable damage on the United States in order to drive it out of the Muslim holy places of the Middle East. His organization, known as Al Qaeda, or the Franchise, had in 1991 volunteered to lead the Islamic effort to force Saddam Hussein to leave Kuwait, but his offer was overlooked by the Saudi royals. Subsequently in exile in the Sudan, and after 1995 in Afghanistan as a guest of the Taliban regime, Osama preached Islamic unity and

defiance in opposing the West's continued military basing in the region and the support it was giving to autocratic and selfish rulers in Saudi Arabia, Egypt, and the Gulf who were doing nothing to provide for their populations. The CIA, in particular in the U.S. intelligence community, became alarmed at the growing strength, sophistication, and appeal of Osama's rhetoric against the United States' role in the Middle East, which targeted it as the "far enemy." After President Clinton's weak and ineffective response to the African embassy bombings, the CIA established a task force to track Osama and Al Qaeda, but it was never able to deliver the knockout punch on his compound in Afghanistan or stop his continuing deadly momentum during the Clinton years, even though then-DCI George Tenet "declared war" on Al Qaeda in an attempt to bring focus to American intelligence's counterterrorist strategy.

In 2001 the CIA began receiving heightened liaison reporting from U.S. allies in Europe and the Middle East that Al Qaeda was planning something big. But where—in the region or against a U.S. installation overseas—was unknown. This was becoming Osama's trademark: long months of preparation and then a sudden strike. But just like the U.S. government's previous experience with a massive surprise attack on U.S. territory at Pearl Harbor, we were not prepared nor really expecting an attack in the continental United States. September 11, 2001, was an unforeseen and life-shattering wake-up call on the capacity of nonstate, religious-inspired terrorism to threaten stable societies like the United States and our European allies. It took President George W. Bush minutes to declare that the United States was involved in a war against terror and that all the military and intelligence resources of the United States would be deployed to win it.

What were those intelligence resources? In late 2001, in what condition did the intelligence community find itself to take on Osama bin Laden, Al Qaeda, and the challenge of religious-based international terror? With the passing of the Cold War, the CIA had been downsized and had in addition witnessed the dramatic departure of large numbers of expert spy handlers and analysts whose skills had been shaped by the challenge of the Soviet Union, and who did not have much interest in and familiarity with the milieu of terrorism, drugs, crime, and weapons proliferation, issues which would be the meat and potatoes of Presidential Decision Directive 35 that set the blueprint for intelligence community targeting after the Cold War ended. So they retired, and took with them their knowledge of spy tradecraft and of foreign languages. On top of that, as the 9/11 post-mortems would show, the intelligence agencies had grown into mature bureaucracies without much initiative, imagination, or creativity. They faced a target that operated in the shadows of nation-states but wasn't one; that had low overhead and a tight network of collaborators that it deployed with iron-handed discipline; and that possessed one unassailable attribute: Many of its adherents were willing to commit suicide for the cause, and would strap on a bomb just to take civilian bystanders with them.

Other problems beset the intelligence agencies in 2001 as well. A division between domestic and international spheres of terrorism no longer existed. A plot

that could begin in a Hamburg mosque or a Madrid suburb could be planned for immediate execution in New York or Washington. The divided responsibilities between the FBI and CIA that historical accident and concern about domestic civil liberties had spawned in the aftermath of World War II were hindrances in the 21st century to the kind of instant information sharing and teamwork that cell phones and Internet access in the hands of our terrorist attackers demanded. Compartmentalization and "need to know" take on sinister meanings when the effect is to deny intelligence to a sister agency equally charged with the responsibility to pre-empt a terrorist act.

Some of the more egregious barriers to intelligence sharing and teamwork between the intelligence agencies were struck down in the USA-PATRIOT Act passed in October 2002, and in the Intelligence Reform Bill, passed in December 2004. Now, wiretap permissions, when granted, run to the individual who is the target of the surveillance, not the instrument by which he intends to communicate. Grand jury testimony in terrorist cases can be shared among the law enforcement and intelligence entities having an interest in the matter. The Foreign Intelligence Surveillance Act (FISA) has been amended to include among the parties against whom the U.S. government may seek authorization for electronic surveillance from the special Foreign Intelligence Surveillance Court not just spies but terrorists as well; and the standard for authorizing surveillance has been broadened to encompass those as to whom terrorism is "a principal purpose" of their activity and not "the" purpose. There are additional sections in the 2001 Act that beef up the anti–money laundering provisions of federal statute and enhance the "sneak and peek" possibilities open to law enforcement, as well as enable more Internet intrusion of suspected terrorists. It is possible that some of the more aggressive portions of the USA-PATRIOT Act may be modified somewhat to include a greater measure of accountability.

The intended changes included in the Intelligence Reform Act of 2004 date back to the Church Committee era but trespassed on more turf, and would only see the light of day three years after September 11, with some of the most intense bureaucratic lobbying of any intelligence bill. In the Act, there has been a concerted effort to remedy one of the principal perceived deficiencies in the performance of the intelligence agencies prior to 9/11, namely the absence of "an attending physician" who could treat the patient as a whole and be responsible for the work of all the specialists racing around performing tests on the patient on their own. That metaphor, used by the 9/11 Commission to sway Congress and the president, was the premise behind creating the new position of Director of National Intelligence (DNI). The DNI was intended to be the intelligence czar, a Cabinet officer holding both managerial and budgetary authority over the entire intelligence community. He would also be the president's principal intelligence adviser.

When the dust settled after passage of the Act, the DNI's lines of command were not as clear as the Commission hoped for. The Defense Secretary and the Department of Defense (DOD) continue to share many of the DNI's management

and budgetary authorities relating to the intelligence agencies under the command of the DOD. The DOD intelligence agencies—NRO, NSA, DIA, and NGA—account for 80 percent of the intelligence budget. There is also the matter of information sharing, which the Act seeks to encourage by requiring the DNI to have a subordinate responsible for creating an information sharing environment in the intelligence community.

The 2004 Act also treats the intelligence community's self-inflicted wounds represented by the failures to warn of the 9/11 attacks and to accurately account for the weapons of mass destruction stockpiled by Saddam Hussein since 1991—believed ready for dispersal to terrorists by Saddam at some point if the UN embargo of Iraq was not lifted. The existence of Iraqi WMD was one of the principal reasons cited by the Bush administration for preparing to go to war against Iraq. A seemingly authoritative National Intelligence Estimate (NIE) circulated by the CIA in October 2002 detailed the supposed holdings of chemical and biological weapons by the Iraqi Ba'athist regime, and the efforts of the regime to make nuclear weaponry advances. Furthermore, United Nations testimony drawn from the NIE by Secretary of State Colin Powell in February 2003, on the eve of the Iraq War, was used to sweep aside Allied opposition to the invasion. It has become painfully clear since that Saddam suspended his WMD programs after 1991 to get out from under the UN-sponsored embargo. There were no WMD stockpiled in Iraq prior to the war, as Saddam had destroyed them.

What made the U.S. intelligence community's views on Iraqi WMD so objectionable was not that they held such preconceptions (most other knowledgeable intelligence services held identical views—the UK, Russia, Germany, France, and Israel), but that the NIE sought to justify the weapons' existence on outdated and unconfirmed reporting. The proprietary data dated from 1991; reports from UN inspectors stopped in 1998; and assessments rested heavily on unilateral sources like "Curveball" whose credibility was in question. The analytical tradecraft employed by the CIA on the critical NIE was fatally deficient.

At the same time, the president's decision to spread the war from Afghanistan to Iraq sounded alarm bells for quite a few veteran intelligence officers within the ranks. A number of these in-house critics believed the move into Iraq would instantly squander goodwill that the American government had gained in the Islamic world as a result of the September 11 attacks. Some intelligence officers subscribed to the view, later corroborated in the post-invasion Iraq Survey Group's two reports, that the inspections broken off in 1998 and the sanctions in place after had already boxed in Saddam.

Moreover, although DCI George Tenet had gained the confidence of the hawks on the president's war cabinet, both Vice President Cheney and Defense Secretary Donald Rumsfeld made it known in the press that they harbored deep distrust of the CIA's analysis of Iraq. The Defense Secretary had steered the 1998 Rumsfeld Commission that took the CIA to task to sharpen its poor nonproliferation reporting, against a backdrop of two missed calls at the Agency in five years—Saddam Hussein's startling WMD advances up to the 1990 Gulf War, and

India's clandestine nuclear tests in 1996. The vice-president possessed quite the opposite disposition, misappropriating even dubious raw intelligence leads to hype the imminent threat from the Ba'athist regime. Analysts at Langley found themselves frozen out of most White House planning. The war cabinet opened a small ad hoc shop within the Defense Department to cherry-pick intelligence reporting from across the community, to be seeded in the media to reinforce two bogus claims: (1) that Iraq's Ba'athists had entered into an active pact with bin Laden's network, and that (2) the Ba'athists were on the verge of going nuclear. The Secretary was known to scorn the DIA's Iraq analysis as well, and he overruled pointed warnings issued by the Army Chief of Staff that the U.S. military could not occupy the country without a contingent of 300,000 soldiers. Amidst rising tensions and mounting controversy over Saddam's alleged possession of nuclear weaponry, Tenet balked too, sending a formal request to the Department of Justice to begin a criminal investigation to identify the source of a leak of a CIA operative's identity (a career officer who was unwittingly dragged into the dispute over the war's strained *casus belli*) even though it was sufficiently clear that the leaker would have to have been a senior White House official.

As the war wore the military down until it was an occupation in disarray, disgruntlement surfaced publicly. First, Richard Clarke, the former counterterrorism czar at the National Security Council made searing statements against the administration at the 9/11 Commission hearings, and then the departing National Intelligence Officer for the Middle East, Paul Pillar spoke out:

> If the entire body of official intelligence analysis on Iraq had a policy implication, it was to avoid war—or, if war was going to be launched, to prepare for a messy aftermath. What is most remarkable about prewar U.S. intelligence on Iraq is not that it got things wrong and thereby misled policymakers; it is that it played so small a role in one of the most important U.S. policy decisions in recent decades.[2]

The overlord at the DIA for Iraq planning, Spider Marks, told a reporter at the *Times* that prewar misjudgments had been made in many quarters, not just in the Cabinet leadership. "We lost our finger on the pulse of the Iraqi people and built intelligence assessments from a distance."[3] Out in Langley, the CIA has been under a pall.

The blunt consensus in the 9/11 Commission report and on Capitol Hill in the Intelligence Reform Act of 2004 to downgrade the CIA was probably not ill-advised. The Agency now has the leeway to be loyal at arm's length during domestic imbroglios, and in principle it has a new referee in the DNI. This has hardly been an auspicious time, however, to watch the demoralization at the CIA, with constant leaking of sensitive intelligence information and the hemorrhaging of experienced intelligence officers into lucrative private-sector security jobs or retirement. Where does that now leave the CIA and the intelligence community, who bear the preponderant responsibility to inform the president about terrorists

and their targets *before* these attacks occur? Future performance alone will provide the answer. The intelligence community has weathered its share of crises in the past. Yet there are some systemic reasons to be concerned.

To start with, the intelligence agencies allowed their capabilities to attenuate markedly during that ten-year period between the disintegration of the Soviet Union and September 11, 2001. There are still too few intelligence officers who have studied and understand Arabic civilizations or who have lived in the Middle East at some point in their careers. Moreover, many of the collection techniques of the Cold War have been rendered obsolete by cell phones, the Internet, and other aspects of changing technology. The CIA cannot continue to operate as it did in the pre-Iraq period, largely excluded from the hard targets that the United States is up against. Where it has no physical presence, the Agency has historically relied for HUMINT primarily on defectors, detainees, legal travelers, opposition groups, and foreign government liaison services, but these sources divulge their secrets at some distance in time and space from the ongoing developments inside the target they are reporting on. Getting inside the adversary's organization is thus a higher priority than it was even in the Cold War. Yet even though the Directorate of Operations budget is now more than double its pre–September 11 levels, an estimated 80–90 percent of intelligence information about Al Qaeda still comes in as SIGINT.[4] The whereabouts, goals, and tactics of terrorists are thus available only imprecisely and intermittently.

In the HUMINT area, American intelligence is still behind other services in having linguists who speak the hard languages of the Middle East, Central Asia, or Southeast Asia. In addition, this assignment is becoming less appealing to spy runners from the standpoint of safety and quality of life. Increasingly, CIA operatives will bring back key intelligence only by acting with the flexibility, the skills, and the cover it takes to run operations unlinked with an official installation—under nonofficial cover. Consequently, the problems spies face conducting espionage will be more dangerous. Families, too, will be divided, as many overseas tours in areas of prime concern to the intelligence agencies are not safe for young children.

Furthermore, there has been an especially rocky post-Tenet transition for the current Director of the Central Intelligence Agency (DCIA), former Congressman Porter Goss. Mr. Goss has been criticized for bringing a number of hostile and inexperienced congressional staffers with him to Langley, making for even more precipitous erosion from the ranks among senior officers with substantial field experience. This will hinder the CIA's ability to take full advantage of the uptick in personnel recruitment, because so many experienced officers appear to be leaving. Goss announced that rebuilding the operations directorate would be the overriding priority of his tenure, but an irony thus far has been the number of critics comparing the present impasse to DCI Stansfield Turner's first year, marked by some of the most severe confrontations and mishandled purges the Directorate had ever experienced. By the end of 2005, Goss had lost one

Directorate of Operations head, two deputy directors, and more than a dozen department, division, and station heads.[5]

An equally fundamental point is that Americans are not the "good guys" any more in many areas of the Middle East. This sounds simplistic, yet much of U.S. intelligence success during the mature stages of the Cold War occurred because Soviet and Soviet Bloc officials volunteered to work for the American or British intelligence services as a way to oppose the corruption and misery of their own lives behind the Iron Curtain. That motivation appears less prevalent in the Middle East today. The United States is perceived as a threatening, non-Islamic outside force, only interested in the region's petroleum resources. Perhaps President Bush's hard push for democratic governments in the region will alter this attitude. It will be a hard sell.

The upshot of pervasive suspicions in the region about American aims is that, to be successful, the CIA and the other intelligence community HUMINT collectors will have to work indirectly, and multilaterally, through the good offices of friendly intelligence services, the operational channels called intelligence liaison. Since September 11 the CIA has been doing that in a major way, trading superior resources and technology for on-the-ground intelligence information about terrorist threats. The CIA has built a formalized network of over two dozen liaison offices, and DOD has gotten into the game as well, with less formal and even lower profile liaison and reconnaissance missions for the special forces. These DOD operations do not fill the need for nonofficial cover and penetrations, but they do have a tactical yield.

The difficulty liaison relationships present, however, is that we are no longer in complete control of the spy operation. Our liaison intermediaries will influence both whom we target and how we manage the take. The result is bound in many cases to be a dilution of the product and a diminished timeliness. But the most worrisome deficiency will be a lack of confidence that one is getting the full picture, with the ongoing potential to leave the United States vulnerable and the region unstable. It is worth remembering the lessons of the Pakistani ISI's control over our access to the *mujahedeen* during the 1980s and 1990s in Afghanistan, or the heavily slanted read of the opposition that the Shah's SAVAK presented the CIA in Iran's prerevolutionary decades. Nevertheless, liaison operations account so far for nearly all of the 3,000 suspected terrorists who have been captured or killed outside the Iraq theater.[6]

Disruptions in these liaison relationships comes with the territory, but the CIA's experiences in Latin American counternarcotics operations have provided a number of relatively useful lessons for working with less corruptible, more trustworthy elite units in the more questionable partnerships with foreign services. Porter Goss has rightly pronounced himself wary of leaning too far toward liaison operations. There are, however, elements of liaison operations that cannot be replaced by CIA HUMINT work. The first of these is legal access: To carry out targeted killings in a foreign country, it becomes prudent to give and receive assurances from other sovereign governments. Kidnapping also is best avoided

wherever the local service is willing to kick down the door for us. And shutting down nearly endlessly reroutable financing pipelines to terrorists requires a willingness to do so on the part of many sovereign partners simultaneously.

The intelligence community's technical collection programs may not be in much better shape than its HUMINT. Signals intelligence gathering is hindered by inadequate translation capabilities, while a wary target will be more willing to communicate by word of mouth, cleft stick, and carrier pigeon, than by telephone or more modern means. From an operational standpoint, the fallout from the brouhaha over warrantless surveillance by the NSA of communications from potential terrorists abroad with individuals in the United States that arose in early 2006 may further limit the gathering of useful intelligence. Actually, it appears that most Al Qaeda instructions are moving through Arabic websites on the Internet, which intelligence services worldwide are not yet recovering or translating in a comprehensive or timely fashion.

When all is said and done, counterterrorism and counterproliferation intelligence gathering follows a new paradigm. It is less about classic espionage than persistent tracking of terrorists and their potential weapons by good detective work and perceptive mining of reams of open sources. This is no longer back-alley skulking in a trench coat. It is down-and-dirty police investigative work, tracing radicals and their bomb-making materials, and recruiting informants to watch mosques and radical meeting sites. That is why in the United States it is so important for the CIA to work well with the FBI, with Customs, with Immigration and Naturalization, and with local police first responders. Intelligence gathering in the 21st century is now less about James Bond or George Smiley than it is a Frankenstein composite of law enforcement, spies, and forensics.

NOTES

The author wishes to express his gratitude to Princeton Woodrow Wilson School Ph.D. candidate Martin Stein who assisted significantly in the preparation of this chapter.

1. Seymour Hersh, "Huge CIA Operation Reported in U.S. Against Antiwar Forces, Other Dissidents During Nixon Years," *New York Times,* December 22, 1974; Hersh, "President Tells Colby to Speed Report on CIA," *New York Times,* December 24, 1974; Hersh, "3 More Aides Quit in CIA Shake-Up," *New York Times,* December 30, 1974.

2. Paul R. Pillar, "Intelligence, Policy, and the War in Iraq," *Foreign Affairs* 85 (March/April 2006), pp. 15–27, at 16.

3. Michael R. Gordon, "Catastrophic Success: Poor Intelligence Misled Troops About Risk of Drawn-Out War," *New York Times*, October 20, 2004.

4. Dana Priest, "Foreign Network at Front of CIA's Terror Fight," *Washington Post*, November 18, 2005.

5. Dafna Linzer, "A Year Later, Goss's CIA Is Still in Turmoil," *Washington Post*, October 19, 2005.

6. Ibid.

6

OPEN SOURCE INTELLIGENCE

ROBERT DAVID STEELE

OPEN SOURCE INTELLIGENCE (OSINT) IS THE ONLY discipline that is both a necessary foundation for effective classified intelligence collection and analysis and a full multimedia discipline in its own right, combining overt human intelligence from open sources, commercial imagery, foreign broadcast monitoring, and numerous other direct and localized information sources and methods not now properly exploited by the secret intelligence community. OSINT is uniquely important to the development of strategic intelligence not only for the government, but for the military, law enforcement, business, academia, nongovernmental organizations, the media, and civil societies including citizen advocacy groups, labor unions, and religions for the simple reason that its reliance on strictly legal and open sources and methods allows OSINT to be shared with anyone anywhere, and helps create broader communities of interest through structured information sharing.

It can be said that at the strategic level in particular, but at all four levels of analysis (strategic, operational, tactical, and technical) generally, the secret intelligence communities of the world are inside-out and upside-down. They are inside-out because they persist in trying to answer important questions with unilaterally collected secrets, rather than beginning with what they can learn from the outside-in: from the seven tribes[1] and the more than ninety nations that form the coalition. They are upside-down, at least in the case of the United States and selected other major powers, because they rely too much on expensive overhead satellite systems instead of bottom-up ground truth networks of humans with deep historical, cultural, and localized knowledge.

In the long-run, I anticipate that OSINT will displace 80 percent of the current manpower and dollars devoted to secret sources and methods, and that

this will offer the taxpayers of the respective nations a return on investment at least one thousand times better than what is obtained now through secret sources and methods. A proper focus on OSINT will alter the definition of "national" intelligence to embrace all that can be known from the seven tribes across both the home nation and the coalition nations, and will dramatically reform intelligence, electoral processes, governance, and the application of the national, state, and local budgets in support of the public interest.

Strategically, OSINT will restore informed engaged democracy and moral capitalism, a new form of communal capitalism, in America and around the world. OSINT is, at root, the foundation for the emergence of the world brain, and the empowerment of the public.

The bulk of this chapter will focus on OSINT and intelligence reform at the strategic level, but it is essential that the reader appreciate the implications of OSINT for electoral, governance, and budgetary reform so as to better realize the enormous implications of the revolution in intelligence affairs[2] for which OSINT is the catalyst.

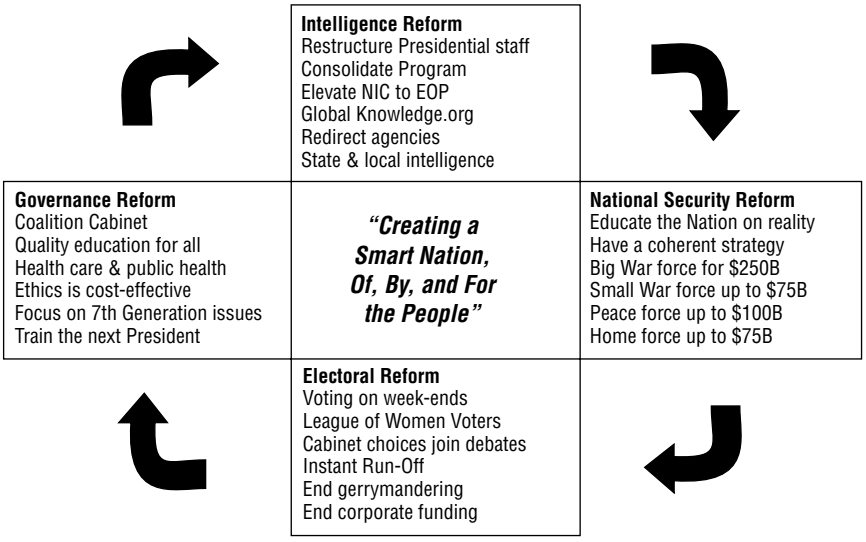


Figure 6-1. Four Strategic Domains for Reform Catalyzed by OSINT

Note: NIC = National Intelligence Council; EOP = Executive Office of the President. It is important to observe that the Global Knowledge organization, now called an Open Source Agency, is intended to be completely independent of both presidential and congressional manipulation. This chart is discussed in more detail in the final section of this chapter on governance reform.

Source: Drawn from "Citizen in Search of a Leader" as prepared 8 January 2003 and posted to http://www.oss.net. Additional detail on each reform domain can be found in that document.

The impetus for reform across all four strategic domains could emerge from within any one of the four. If the economy collapses and the war on Iraq combined with an attack on Iran cause a clear and present danger to emerge in the form of global Islamic counterattacks that are asymmetric and indiscriminate as well as widespread, we can anticipate not just the ejection of the extremist Republicans, but also of the complacent and equally corrupt and ignorant Democrats.[3]

There is a growing awareness within the public, described by some as "smart mobs," or "wisdom of the crowds," or—our preferred term—collective intelligence, that it is now possible for individuals to have better intelligence based on open sources and methods, that is being made available to, or acknowledged by, the president.[4] We will see, within the next four years, a dramatic increase in both historical accountability[5] and current accountability for actions impacting on future generations and other communities.

Electoral reform will be inspired by citizens realizing that both the Republican and Democratic parties have become corrupt as well as inept at representing the public interest.

Governance reform will be inspired by citizens realizing that in today's world, we need a networked model of governance that elevates intelligence to the forefront. Decisions must be made in the public interest and be sustainable by consensus and conformance to reality, not purchased by bribery from special interests who seek to loot the commonwealth and/or abuse their public power to pursue the ideological fantasies of an extremist minority.

Budgetary reform will be inspired by citizens who understand that we still need to be able to defend ourselves, but that waging peace worldwide is a much more cost-effective means of both deterring attacks and of stimulating sustainable indigenous wealth that is inherently stabilizing.

OSINT AND INTELLIGENCE REFORM

Open source intelligence (OSINT) should be, but is not, the foundation for all of the secret collection disciplines, and it could be, but is not, the foundation for a total reformation of both the governmental function of intelligence and the larger concept of national and global intelligence, what some call collective intelligence or the world brain.[6]

Secret intelligence, inclusive of covert action and counterintelligence, has failed in all substantive respects since the end of World War II and through the Cold War. In failing to meet the mandate to inform policy, acquisition, operations, and logistics, secret intelligence has contributed to the "50 Year Wound"[7] and failed to stimulate a redirection of national investments from military capabilities to what General Al Gray, then-Commandant of the Marine Corps, called "peaceful preventive measures."[8]

Secret intelligence became synonymous with clandestine and secret technical collection, with very little funding applied to either sense-making information

technologies, or to deep and distributed human expertise. The end result at the strategic level can be described by the following two observations, the first a quote and the second a recollected paraphrase: Daniel Ellsberg speaking to Henry Kissinger: "The danger is, you'll become like a moron. You'll become incapable of learning from most people in the world, no matter how much experience they have in their particular areas that may be much greater than yours" [because of your blind faith in the value of your narrow and often incorrect secret information].[9] Tony Zinni speaking to a senior national security manager: "80% of what I needed to know as CINCENT I got from open sources rather than classified reporting. And within the remaining 20%, if I knew what to look for, I found another 16%. At the end of it all, classified intelligence provided me, at best, with 4% of my command knowledge."[10]

Secret intelligence may legitimately claim some extraordinary successes, and we do not disagree with Richard Helms when he says that some of those successes more than justified the entire secret intelligence budget, for example, in relation to Soviet military capabilities and our countermeasures.[11] However, in the larger scheme of things, secret intelligence failed to render a strategic value to the nation, in part because it failed to establish a domestic constituency, and could be so easily ignored by Democratic presidents and both ignored and manipulated by Republican presidents.[12]

In this first section, we will briefly review both the failings of each aspect of the secret intelligence world, and summarize how OSINT can improve that specific aspect.

History

The history of secret intelligence may be concisely summarized in relation to three periods:

1. *Secret War.* For centuries intelligence, like war, was seen to be the prerogative of kings and states, and it was used as a form of "war by other means," with spies and counterspies, covert actions, and plausible deniability.[13]

2. *Strategic Analysis.* During and following World War II, Sherman Kent led a movement to emphasize strategic analysis. Despite his appreciation for open sources of information, and academic as well as other experts, the clandestine and covert action elements of the Office of Strategic Services (OSS) and the follow-on Central Intelligence Group (CIG) and then Central Intelligence Agency (CIA), grew out of control, well beyond what President Harry Truman had envisioned when he sponsored the National Security Act of 1947.[14]

3. *Smart Nation.* Since 1988 there has been an emergent movement, not yet successful, but increasingly taking on a life of its own in the private sector. Originally conceptualized as an adjunct to secret intelligence, a corrective focus on open sources long neglected, it was soon joined by the collective intelligence movement that has also been referred to as "smart mobs" or "wisdom of the crowds," or "world brain." H. G. Wells conceptualized a world brain in the

1930s. Quincy Wright conceptualized a world intelligence center in the 1950s. Others have written about smart nations, collective intelligence, global brain, and the seven tribes of intelligence.[15]

Although the U.S. intelligence community has individuals that respect the value of open sources of information, and every major commission since the 1940s has in some form or another called for improved access to foreign language information that is openly available, the reality is that today, in 2006, the United States continues to spend between $50 billion and $70 billion a year on secret collection, almost nothing on all-source sense-making or world-class analysis, and just over $250 million a year on OSINT. This is nothing less than institutionalized lunacy.

The future history of secret intelligence is likely to feature its demise, but only after a citizen's intelligence network is able to apply OSINT to achieve electoral, governance, and budgetary reform, with the result that secret intelligence waste and defense acquisition waste will be converted into "waging peace" with peaceful preventive measures and a massive focus on eliminating poverty, disease, and corruption, while enabling clean water, alternative energy, and collaborative behavior across all cultural boundaries.[16]

Requirements

Requirements, or requirements definition, is the single most important aspect of the all-source intelligence cycle, and the most neglected. Today, and going back into history, policy makers and commanders tend to ignore intelligence, ask the wrong questions, or ask questions in such a way as to prejudice the answers. There are three major problems that must be addressed if we are to improve all-source decision support to all relevant clients for intelligence:

1. *Scope.* We must acknowledge that all levels of all organizations need intelligence. We cannot limit ourselves to "secrets for the president." If we fail to acknowledge the needs of lower-level policy makers, including all Cabinet members and their Assistant Secretaries; all acquisition managers; all operational commanders down to civil affairs and military police units; all logisticians; and all allied coalition elements including nongovernmental organizations, then we are not being professional about applying the proven process of intelligence to the decision-support needs of key individuals responsible for national security and national prosperity.

2. *Competition.* We must acknowledge that open sources of information are vastly more influential in the domestic politics of all nations, and that it is not possible to be effective at defining requirements for secret intelligence decision-support in the absence of a complete grasp of what is impacting on the policy makers, managers, and commanders from the open sources world (see Figure 6-2).

3. *Focus.* Third, and finally, we must acknowledge that, at the strategic level, our focus must of necessity be on long-term threats and opportunities that are global, complex, interrelated, and desperately in need of public education, public

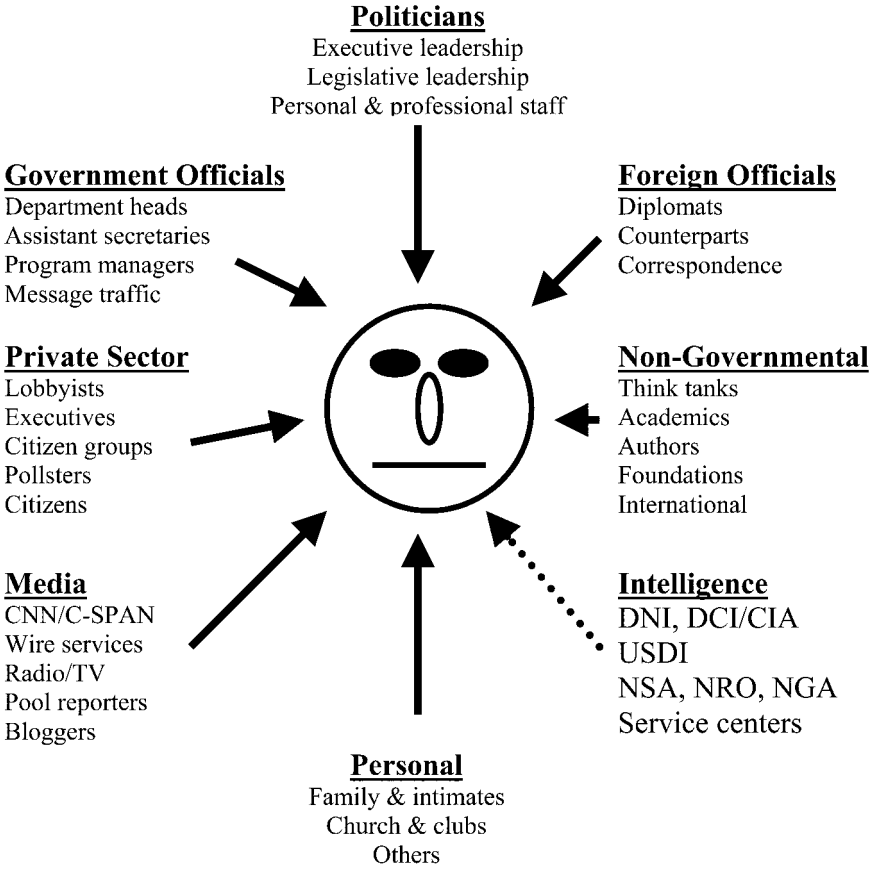


Figure 6-2. Competing Influences on the Intelligence Consumer

recognition, and public policy that is sustainable, which is to say, nonpartisan or bipartisan. Consider, for example, the findings shown in Figure 6-3 from the Report of the High-Level Panel on Threats, Challenges and Change, *A More Secure World: Our Shared Responsibility.*[17]

The average utility and relevance of OSINT to the global threats shown in Figure 6-3 is—on the basis of my informed estimate—82.5 percent, which comes very close to the generic "80-20" rule. We must conclude that any nation that persists in spending 99.9 percent of its intelligence funds on collecting secrets,[18] and less than one half of one percent of its intelligence funds on OSINT, is quite literally clinically insane (or insanely corrupt) at the highest levels.

In all three of the above cases, only OSINT can deliver a solution that is affordable, practical, and infinitely shareable with all stakeholders both in and out of government.

Economic and social threats, including	**95%**
• poverty	99%
• infectious disease	95%
• environmental degradation	90%
Interstate conflict	**75%**
Internal conflict, including	**90%**
• civil war	80%
• genocide	95%
• other large-scale atrocities	95%
Nuclear, radiological, chemical, and biological we	**75%**
Terrorism	**80%**
Transnational organized crime	**80%**

Figure 6-3. OSINT Relevance to Global Security Threats

Collection

Secret collection has made three fundamental mistakes across several generations of management:[19]

1. *Denigrated OSINT.* It chose to ignore open sources of information, assuming that the consumers of intelligence were responsible for their own OSINT, and that OSINT would not impact on secret collection. In fact, OSINT can dramatically reduce the cost and the risk, and increase the return on investment in secret sources and methods, simply by helping with targeting, spotting, assessment, validation, and the overall strategic context of what needs to be collected "by other means." It merits very strong emphasis that this failure to respect open sources of information falls into three distinct forms:

- Complete disrespect for history in all languages. There is no place within the U.S. government where one can "see" all Chinese statements on the Spratley Islands, or all Iranian statements on the competing Caliphate concept, or all Brazilian statements on alternative energy sources. We simply do not compute history, and consequently what little we know about current events and threats is known in isolated ignorance of history.

- Complete abdication of any responsibility for monitoring, understanding, and engaging substate or transnational entities as major factors in international affairs, and as threats or potential allies in domestic security and prosperity.
- Finally, almost complete abdication for more nuanced topics other than standard political-military calculations, with very important sustained failures to collect information on socioeconomic, ideocultural, technodemographic, or natural-geographic matters. This has been compounded by an extraordinary laziness or ignorance in relying almost exclusively on what can be stolen or obtained readily in English—the United States simply does not "do" the key 31 languages,[20] much less the totality of 185 languages necessary to understand the substate threat and the global network of cause and effect.

2. *Official Cover.* We have relied almost exclusively, at least in the United States, on "official cover" for our spies, and known trajectories for our satellites. Non-Official Cover (NOC), which does not offer any form of diplomatic or other official immunity from incarceration or eviction, has been treated as too expensive, too complicated, and not worthy of full development. The result has been the almost total compromise of all U.S. secret agents and case officers overseas, as well as their varied not-so-secret thefts of the codebooks of other nations. We not only don't know what we don't know, we are in denial about the basic fact that what we do know has been compromised.

3. *Failure to Process.* Finally, and this applies to both clandestine human collection and secret technical collection, we have failed, with deliberate ignorance at the management level, to devote any resources of significance to processing—to sense-making. Today, eighteen years after the needed functionalities for an all-source analytic desktop toolkit were published, we still do not have a desktop analytic toolkit. Today, despite major advances in the private sector with respect to machine-speed translation, and machine-speed statistical, pattern, and predictive analysis, the large majority of our classified intelligence analysis is still done the old-fashioned way: reading at human speed, cutting and pasting, attempting to make sense of vast volumes of secret information while lacking equivalent access to vast volumes of open source information (and especially open source information in any language other than English), limited by the physics of the twenty-four-hour day.

OSINT combines the proven process of intelligence with the ability to collect, process, and analyze all information in all languages all the time. We collect, at best, 20 percent of what we need to collect, at 99 percent of the cost, and we spill most of that for lack of processing capabilities. It can be said, as an informed judgment, that Washington is operating on 2 percent of the relevant strategic information necessary to devise, implement, and adjust national strategy.[21] We should not be sending spies where schoolboys can go, nor should we be ignoring scholarship in all languages.

There will still be a need for selected clandestine human operations, especially against organized crime and translation terrorist groups, but they will need to shift toward NOC and multinational task forces. Secret technical collection will need to emphasize commercial collection first, dramatically refocus secret collection, and shift the bulk of the future resources toward processing—making sense of what we do collect—and toward close-in technical collection inclusive of beacons for tracking bad guys and bad things.

Collection management will require draconian reform. Instead of defaulting to the tasking of secret collection capabilities, an enlightened collection manager will first determine if they can *find* the information for free in their existing stores of knowledge; then determine if they can *get* the information for free from an allied government or any of the seven tribes; and then determine if they can *buy* the information from a commercial provider, ideally a localized provider with direct indigenous access, in the time and with the operational security (e.g., cover support plans) appropriate to the need. Only if the first three options are unsuited to the need should the collection manager be tasking secret sources and methods, and even that will have to change to accommodate new possibilities from multinational secret task forces able to leverage the collection capabilities of varied countries, many of them vastly superior to the United States when it comes to both deep-cover clandestine human penetrations, and the related ability to place close-in secret technical collection devises.[22]

OSINT is, without question, the catalyst for a revolution in how we collect intelligence.

Processing

Apart from our failure to actually invest in processing (known within the U.S. intelligence community as Tasking, Processing, Exploitation, and Dissemination, or TPED), we have made three consistent mistakes over time that have made it virtually impossible, and now unaffordable, to actually do automated all-source analysis:

1. *No Standards.* We failed to establish data standards that could be used at the point of entry for both secret and open sources of information. This applies to both information sources and information software. Not only was the intelligence community much too slow to adopt commons standards such as eXtended Markup Language (XML), Resource Description Framework (RDF), Web Ontology Language (OWL), and Simple Object Access Protocol (SOAP), today it is either ignorant of or reluctant to move ahead aggressively with Open Hypertextdocument System (OHS)[23] and eXtended Markup Language Geospatial (XML Geo). The obsession with security, and the pathology of limiting contracts to the established firms in the military-industrial complex who profit from proprietary software and human headcount rather than real-world low-cost answers, can be blamed for the chasm between the secret intelligence world and the real world of open sources and standards.

2. *No Geospatial Attributes.* In fall 1988 it was made known to the U.S. intelligence community and clearly articulated by the author to a meeting of the General Defense Intelligence Program (GDIP), that in the absence of geospatial attributes for every datum entering the all-source processing system (actually an archipelago of private databases), that machine-speed all-source analysis and fusion would be an impossibility. Despite this, the individual secret collection disciplines of clandestine human intelligence (HUMINT), signals intelligence (SIGINT), and imagery intelligence (IMINT) refuse to do anything other than persist with their human analytic reporting that provides date-time-group (DTG) and geographic place names where known, but no standard geospatial attributes for relating information to a map. Today Google Earth is being used in extraordinary ways to visualize relationship databases of real estate, shipping, and other important topics, and the individual citizen is light years ahead of the average "cut-and-paste" analyst at the federal, state, and local levels.

3. *No Integration.* There is no single place where all known information comes together. Despite critical concerns raised by every congressional and presidential commission since the 1940s, the U.S. intelligence community has continued to be "flawed by design"[24] and has persisted in the turf wars between the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI), between the FBI and the Drug Enforcement Administration (DEA), between the FBI and the Department of Justice (DoJ), and between the Departments of State and Defense. Within the Department of Defense (DoD), the services have not only competed with one another but actively conspired to fabricate and manipulate intelligence to exaggerate the threats relevant to their budget share. A corollary of this abysmal situation is that processing within the stovepipes has been focused on the delivery of documents rather than on making sense of all of the information in the aggregate. With the exception of selected efforts at the National Security Agency, the Army's Intelligence and Security Command, and the U.S. Special Operations Command, virtually all civilian and military analysts are still in cut-and-paste mode, and do not have the tools for pattern or trend analysis or anomaly detection, much less predictive analysis.

In processing, it is machine speed translation and statistical analysis, based on standards and global distributed information integration, that permits early warning, anomaly detection, and structured analysis that can be completed in a timely—that is to say, relevant—manner. OSINT is where the real innovation is occurring, and I anticipate that within ten years the secret world will be sharply restricted to no more than 20 percent of its present cost and size, while the balance of the funding is redirected to a mix of OSINT that can be shared with anyone, with peaceful preventive measures in lieu of a heavy-metal military.

Among the corrective measures required in secret processing, which OSINT will facilitate, are a shift toward the Internet as the common operating environment; the adoption of open source software to provide a generic access and collaborative sharing environment for all seven tribes;[25] the development of 24/7 "plots" at every level of governance in which all information can be seen in time

and geospatial context;[26] and the creation of a national skunkworks with an antitrust waiver for the public testing and certification of all open sources, software, and services. Rapid promulgation of free wireless within urban areas and in the Third World will help accelerate both sharing in the North and West, and uploading of useful information from the East and South.

Analysis

In evaluating the failure of analysis, it is important to understand that most U.S. analysts are too young, too inexperienced in the real world, and too isolated from foreign or even U.S. private-sector experts, to realize that the secret information they are receiving is out of context, often wrong, and largely irrelevant to strategic analysis. Their managers are too busy trying to be promoted or to win bonuses or please the White House (or the representative of the White House, the Director of Central Intelligence [DCI]). As a result, the strategic analysis vision of Sherman Kent has been dishonored and largely set aside. There have been three major failures in analysis over time.

1. *Hire Young.* The intelligence management philosophy in both the national civilian hires and at the military theater and service center levels has combined "hire to payroll" with obsessive lazy security parameters that have resulted in an analytic population that is largely young, white, and mostly bereft of overseas experience and especially long-term residency in foreign countries. Budgets have been used to hire low and promote over time, treating analysis as an entry-level hiring challenge rather than a mid-career sabbatical challenge. This has been deeply and pathologically influenced by a low-rent security philosophy that has combined paranoia over foreign contacts (and relatives) with an unwillingness to spend the time and thoughtfulness necessary to clear complicated individuals who have led complicated lives. This personnel management failure stems from the larger philosophical management failure, which confuses secrets with intelligence, and thus demeans expertise from the open source world while assuming that young analysts will succeed because they have access to secrets, rather than because of any application of analytic tradecraft such as might take twenty years to refine.

2. *Hard Target Focus.* In keeping with the military-industrial complex and its desire to profit from the Cold War, the national and military intelligence communities devoted virtually their entire budgets and most of their manpower to the "hard targets" (generally, Russia, China, Iran, India, Pakistan, Libya, and—hard to believe, but true—Cuba). They ignored all of the "lower tier" issues and Third World countries,[27] and also focused only on very big threats, not on very big opportunities for peaceful preventive measures where a few dollars invested in the 1970s might have eradicated Anti-Immune Deficiency Syndrome (AIDS) or dependency on Middle Eastern oil. This was of course in keeping with policy preferences, and even when the CIA did excellent work (for example, accurately forecasting the global AIDS epidemic), it could safely be ignored because its

work was not available to the public or even to most members of Congress. A very important consequence of this narrow focus was the complete failure to ensure that all of the sources of national power—diplomatic, informational, military, economic (DIME)—were funded, acquired, fielded, and applied in a coherent and timely manner. The entire military-industrial-intelligence complex has been skewed toward a heavy-metal military—a few big platforms or big organizations—that are only relevant 10 percent of the time. We are not trained, equipped, or organized for small wars, waging peace, or homeland defense. This is still true—truer that ever—in the aftermath of 9/11 and the invasions and occupations of Afghanistan and Iraq.

3. *Local Now.* Finally, U.S. intelligence (and many foreign intelligence communities) focused on the local now instead of the global future. "Current intelligence" dominated the *President's Daily Brief* (PDB), and over time longer term research fell by the wayside. This problem was aggravated by a draconian editing process in both the national civilian and theater- or service-level military, where a twelve-month research project could be subject to eighteen-month editing cycles, such that the work was out of date or thoroughly corrupted by the time it was finally released to a relatively limited number of policy makers. With most of the intelligence products being released in hard copy, or messages that were printed out and not saved electronically, the overall impact of U.S. intelligence production, and especially Codeword production, must be judged as marginal.[28]

OSINT is "the rival store."[29] Whereas I spent the first eighteen years of my campaign to foster an appreciation on OSINT and focusing on the urgency of integrating OSINT into secret sources toward improved all-source analysis, I plan to spend the next eighteen years burying 80 percent of the classified world. They are too expensive, too irrelevant, and pathologically antithetical to the new and correct Swedish concept of Multinational, Multiagency, Multidisciplinary, Multidomain Information Sharing (M4IS).[30] OSINT analysis will in the future be the benchmark by which classified sources and methods are judged to be relevant and cost-effective, or not. The Director of National Intelligence (DNI) has chosen to remain focused on secrets for the president. So be it. OSINT, from a private-sector and nongovernmental foundation, will capture all the other consumers of intelligence. The day will come when "clearances" are severely devalued and open source access—international open source access in all languages all the time—is ascendant. The DCI must serve all levels of the government, all seven tribes, and must balance between open and closed sources so as to inform decision makers—and their publics—in order to preserve and enhance the long-term national security and prosperity of the United States. Secret sources and methods—and the existing military—have demonstrably failed in both regards.

Analytic tradecraft notes are available online and should be consulted.[31] All-source analysts should not be hired until they have first proven themselves as masters of all open sources in all languages relevant to their domain and not be considered for mid-career hire unless they are one of the top twenty-five cited

authorities in the field. They must know how to leverage their historian, their librarian, and the Internet. They must know how to identify and interact with the top 100 people in the world on their topic, regardless of citizenship or clearances. Finally, they must understand that they are—and must be trained to be—managers of customer relations and requirements definition, of open sources, of external experts, and of classified collection management. Analysts must know and practice the "new rules" for the new craft of intelligence, with specific reference to being able to actually do forecasting, establish strategic generalizations, and drill down to the neighborhood and tribal levels, not simply hover at the nation-state level.[32]

Covert Action

Covert action consists of agents of influence, media placement, and paramilitary operations. Covert action assumes two things that may once have been true but are no longer true: that an operation can be carried out without its being traced back to the United States as the sponsor, and that the fruits of the operation will be beneficial to the United States. In each of these three areas, the United States has acted with great disdain for the normal conventions of legitimacy, accountability, morality, and practicality, and today the United States is suffering from what is known as "blowback"—it is reaping the dividends from decades of unethical behavior justified in the name of national security but unfounded upon any substantive grasp of long-term reality.

1. *Agents of influence* are individuals bribed covertly who are charged with getting their governments or organizations to pursue a course of action that the United States deems to be necessary but that may not be in the best interests of the indigenous public or its government. Regardless of what one may think of the local country and its government and public, what this really means is that agents of influence are responsible for disconnecting local policies from local realities, and imposing instead a reality or choice selected by the U.S. government. This is inherently pathological. There are certainly some success stories—support to Solidarity in Poland, for example, but this was a capitalization on the fall of communism, not the cause.
2. *Media placement* uses individuals, generally foreign journalists, who are bribed covertly to create and publish stories that communicate an alternative view of reality, one sanctioned by the U.S. government but generally at odds with the actual facts of the matter. There is a constructive side to media placement, for example the promulgation of information about atrocities committed by dictators or Soviet forces, but generally the U.S. government supports most of the dictators it deals with, and reserves this tool for deposing individuals that dare to oppose predatory immoral capitalism or virtual colonialism. Consequently, most media placement

activities consist of propaganda seeking to manipulate rather than deliver the truth. Media placement by spies should not be confused with public diplomacy by diplomats or strategic communication by the military—the latter two are overt truth-telling missions, although misguided practitioners may occasionally stray into propaganda and the manipulation of the truth.[33]

3. *Paramilitary operations* are not only direct assaults on the sovereignty of other nations, but they tend to bring with them black markets, drug running, money laundering, corruption, and the proliferation of a culture of violence and the small arms with which to do indiscriminate violence. The Phoenix program of assassinations in Vietnam, the support to the *contras* and the mining of the Nicaraguan harbors (an act condemned by the World Court), the arming of the Islamic fundamentalists for jihad in Afghanistan, join the planned overthrows of the governments of Chile, Guatemala, Iran, as causes of long-term and costly "blowback." Of all of these, Iran is the most interesting. Had we allowed the nationalization of the oil in Iran and the fall of the Shah, we might today have both a nonfundamentalist Iran as a bulwark against the radicals from Saudi Arabia, but we might also be less dependent on oil, and less subject to the whims of the extraordinarily corrupt Saudi regime and its U.S. energy company allies.

OSINT is the antithesis of all three forms of covert action. As David Ignatius noted so wisely in the 1980s, overt action rather than covert action delivers the best value in both the short and the long run. Promulgating the tools for truth—cell phones, wireless access, access to the Internet—is a means of fostering informed democracy and responsible opposition. It is also a means of creating stabilizing indigenous wealth. OSINT provides a historical and cultural foundation for achieving multicultural consensus that is sustainable precisely because it is consensual. As Jonathan Schell documents so well in *The Unconquerable World: Power, Nonviolence, and the Will of the People*, there are not enough guns in the world to force our way or protect our borders.[34] Only by fostering legitimacy, morality, charity, and full participation of all can we stabilize the world to the mutual benefit of the United States and the rest of the world.

OSINT, in addition to being vastly superior to covert action as a means for establishing reasonable goals that are sustainable over time, is also very well suited to documenting the extraordinary costs of historical covert actions. Only now is the public beginning to understand the lasting damage caused by the U.S. sponsorship of assassination attempts against Fidel Castro, capabilities that were ultimately turned against the unwitting president, John F. Kennedy, and his brother Robert. We have sacrificed our national values and our international credibility at the alter of covert action, and we are long overdue for a deep "truth and reconciliation" commission that evaluates the true costs of covert action, and

that then defines much more narrowly the conditions and protocols for engaging in covert action in the future.

Counterintelligence

Strategic counterintelligence is completely distinct from tactical counterintelligence.[35] In strategic counterintelligence, one is looking for emerging threats at the strategic level, not individual penetrations of specific organizations. This is an area where OSINT should, but does not, shine. The U.S. intelligence community—and consequently the U.S. policy community—have completely missed the end of cheap oil, the end of free water, the rise of bin Laden, and the rise of pandemic disease, even global warming, precisely because national counterintelligence was focused obsessively on penetrating foreign security services, and not on the strategic environment where natural and other threats of omission and commission were to be found. There are three areas in which strategic counterintelligence can benefit considerably from comprehensive OSINT, inclusive of the digitization and statistical analysis of all available historical information.

1. *National Education.* Thomas Jefferson said, "A Nation's best defense is an informed citizenry." This is absolutely correct, and even more so today, when central bureaucracies are no match for agile networked transnational groups. The United States has failed to understand the strategic implications of its lack of border control, its mediocre educational system designed to create docile factory workers, and the trends toward obesity, insularity, and indifference that characterize the bulk of the population today. We have gone hollow for lack of focus.

2. *Environment.* The Singapore military was stunned by the emergence of Severe Acute Respiratory Syndrome (SARS), but unlike the U.S. military they understood it. They realized they were responsible for defending Singapore against all threats, not just manmade or man-guided threats, and added national health and border security against airborne, waterborne, and human- or animal-borne diseases, to their charter. Similarly, the Singapore police have an extraordinarily nuanced and enlightened understanding of their global and regional information needs and responsibilities in relation to deterring and resolving all forms of crime impacting on Singapore. In the United States, and globally with dire consequences for the United States, there are threats associated with the environment and how it changes (including water, energy, and raw material resources) that are simply not understood, not acknowledged, and not being acted upon responsibly by any U.S. administration, be it Democratic or Republican.[36]

3. *Ideology.* There are two ideological threats to U.S. security today, one external, the other internal. The two together are very troubling. Externally, the radical and violent fundamentalist stream of Islam has been armed and energized by jihad in Afghanistan, in Chechnya, and in Iraq. Other small jihads in Indonesia, the Philippines, and southern Thailand, as well as selected locations in Muslim Africa, add to this threat. Internally, U.S. Christian fundamentalists have

assumed a terribly excessive importance in extremist Republican circles, in part because the Texas corporate energy interests chose to make common cause with them. The Middle East, oil, and the almost cultlike extreme religious right have hijacked American democracy. The American left, nominally but not intelligently led by the Democratic Party (which is as corrupt as the Republican Party, but more inept), meanwhile, abandoned faith and God and the sensible calming effect of religion as a foundation for community and ethics.[37] The American ideology of capitalism has also been corrupted. Immoral predatory capitalism, and pathologically inept formulas for "developmental economics" as imposed on failed states by the International Monetary Fund (IMF) and the World Bank have given rise to populism and other forms of indigenous resistance now witting of the collusion between their corrupt elite and immoral foreign capitalism that are in combination looting the commonwealth of many peoples.[38]

In all three of these cases, OSINT has an extraordinary role to play. Under the leadership of Congressman Rob Simmons (CT), a moderate Republican with an extraordinarily deep background in both intelligence and on the Hill, the campaign continues for a national Open Source Agency funded at $3 billion per year, under the auspices of the Department of State (as a sister agency to the Board of Governors that controls the Voice of America and other public diplomacy outlets). However, fully half the budget is intended to fund fifty Community Intelligence Centers and networks across the country (each receiving $30 million at full operating capability). These centers are needed for two reasons: first, to provide 119 and 114 numbers for citizen mobilization (119 alerts all cell phones within a 5 kilometer radius) and citizen neighborhood watch inputs (114 receives cell phone photos, text messages, any form of information, all with geospatial and time tags); and second, to serve as dissemination nodes for transmitting to all schools, chambers of commerce, churches/synagogues/mosques, labor unions, civil advocacy groups, and so on, the wealth of "real world" information to be collected, processed, and shared, free via the Internet, by the Open Source Agency. This will impact very favorably on the environment, as these centers will help citizens at the county, state, and regional levels understand, with precision, where each of them stands with respect to access to clean water, alternative energies and related lifestyle choices, and global threats to their children and grandchildren based on easy access to the actual U.S. federal budget in relation to real world threats and needs. Militarism can be reduced, poverty and disease can be eliminated, and the United States can rejoin the community of nations as a force for good. Finally, all competing ideologies can be subject to scrutiny and understanding, and the majority of Americans who are not part of the right can come together consensually to limit the damage these people can do to the republic, while also holding their political and corporate allies accountable for serving America as a whole rather than a fringe element.

Dramatically redirecting national intelligence toward OSINT will substantially reduce the cost of secrecy, estimated by the Moynihan Commission as being on the order of $6 billion a year (probably closer to $15 billion a year

today),[39] and will also eliminate perhaps 70 percent of the costs associated with establishing the trustworthiness of individuals being considered for clearances. The security and clearance system of the U.S. government is broken beyond repair. Not only does it take over two years for most investigations to be completed, but they are generally substandard investigations that go through the motions and generally do not detect basic aberrations, such as a fascination with child pornography and online molestation of children, as was the case recently with a senior manager in the Department of Homeland Security. The fact is that most sheriffs and other state and local officials are not "clearable" for a variety of reasons, and we may as well recognize that not only is OSINT better suited for most national intelligence information sharing, but we really do not need most of the grotesquely expensive and dysfunctional top-secret "compartments" (over 400 of them, half in the civilian world and half in the military world) and all the attendant costs, including the costs of ignorance stemming from compartmentalized information not being shared. At least at the strategic level we need a national intelligence system in which we are less concerned about betrayal from within, and more focused on emerging strategic threats to our long-term security and prosperity, threats that must not be limited to manmade capabilities, but include animal-borne diseases and other environmental conditions that tend to be shut out from national security decision processes.

Accountability, Civil Liberties, and Oversight

As all of the preceding sections should have made clear, OSINT is the essential contributing factor to dramatically improving the accountability and oversight of the U.S. intelligence community and the policy makers, acquisition managers, and operational commanders who respond to White House direction. OSINT is also a means of dramatically enhancing not just civil liberties, but civic engagement in the practice of democracy. By providing citizens at every level with structured OSINT on any issue for any zip code or other geographic grouping, and by making it possible for citizens to immediately connect with other like-minded citizens and with accountable officials, OSINT in practice is an enabler of a new form of constant engaged informed democracy. Civil liberty infractions will be broadcast or podcast, rapidly aggregated, and civil pressure brought to bear. By harnessing citizens as part of the "home guard" and empowering them with immediate and understandable access to indications and warning information, we will dramatically improve the reporting of relevant information, and—through the Community Intelligence Centers—be able to process, make sense of, and act on or discount the "bottom up" dots that I am convinced will comprise at least 50 percent of the relevant dots needed to prevent the next 9/11.

It is also important to emphasize that, at the strategic level, we need to be concerned not just with accountability and oversight of secret intelligence, but with the much larger issue of whether Congress and the Executive are being responsible in representing the public interest. For this reason are included very brief but vital

sections at the end of this chapter on OSINT and electoral reform, governance reform, and budgetary reform. OSINT is the ultimate resource for citizens to hold their government accountable, and to protect their civil liberties over time.

Strategic Warning

Although the CIA has done some fine work on global threats, and I particular like the work done under John Gannon as Assistant Director of Central Intelligence for Analysis & Production (*Global Trends 2015*, which led to *Global Trends 2020*),[40] on balance the U.S. intelligence community has failed abysmally at strategic warning because of some fundamental operational and philosophical failures.[41]

Operationally, despite fifty years of extraordinarily generous funding for multi-billion-dollar satellite systems, the U.S. intelligence community still cannot do wide area surveillance, real-time change detection, or "the last mile" inclusive of seeing into an urban area, under jungle canopy, and into the deep ravines of mountainous terrain.

Philosophically U.S. intelligence has been a disaster in strategic terms. The cult of secrecy limited "intelligence" to "secrets for the president" and left everyone else, from Cabinet-level leaders to military acquisition manager and operational commanders, to governors and mayors, completely without "decision-support." Perhaps worse, the U.S. intelligence community has refused to recognize the seven tribes of intelligence, shutting out, for the most part, state and local officials with overseas knowledge, business travelers, academics, nongovernmental observers, journalists, labor union leaders, religious travelers, and so on. The obsession with government secrecy over public sharing has cost this nation fifty years of time—the one strategic factor that can be neither bought nor replaced[42]—and at least 3 billion souls of goodwill. U.S. intelligence is a small part of the overall federal government, and it merits comment that most of our problems today cannot be blamed on U.S. intelligence as much as on a corrupt Congress and Executive all too eager to ignore, for example, the Peak Oil warnings of 1974–79 in order to keep the bribes going and the public docile. This is not, however, to excuse the U.S. intelligence community, in as much a focus on OSINT from 1988 onwards would have done much to illuminate and correct the policy errors that benefited from secrecy, obscurity, and public inattentiveness.

Strategic Sharing

The U.S. intelligence community is incapable today, five years after 9/11, of creating a single consolidated watch list of suspected terrorists. The U.S. government as a whole is incapable of sharing everything that it knows for lack of collaborative mindsets, willing management, interoperable systems, and coherent data sets. There are three primary impediments to the U.S. intelligence community ever being able to share readily:

1. *High Side Security.* The obsession with security is occasioned in part by the fact that the secret intelligence world, even though it has "compartments," has never learned to disaggregate secret from nonsecret information. Everything is stored at the "high side," at the highest possible level of security, meaning that nothing can be shared with anyone who is not cleared for the highest level of security, however unclassified the information might be.

2. *Third Party Rule.* The secret world has for decades operated under a "third party rule" that prohibits the sharing of any information received from one party with another party. This rule is extremely detrimental to multilateral sharing, and imposes enormous time, manpower, and dollar costs when something needs to be shared and the sharing must be coordinated. The default condition of the secret world is "do not share."

3. *Legacy Systems.* As John Perry Barlow noted in an article in *Forbes*,[43] if you want to see the last remnants of the Soviet Empire, go visit the CIA and look at their computer systems. The U.S. intelligence community as a whole is still mired in 1970s technology managed by 1950s mindsets, totally out of touch with 21st-century information networks, both machine and human.

OSINT is going to be the catalyst for M4IS and strategic sharing. OSINT is the only discipline that can easily distribute the collection, processing, and analysis burden across all coalition nations (i.e., the ninety nations comprising the U.S. Central Command coalition), and also the only discipline whose products can easily be shared with nongovernmental organizations as well as state and local authorities all over the world who will never qualify for "clearances." It will be our challenge in the next eighteen years to develop an alternative global intelligence community that relies almost exclusively on "good enough" open sources, and that consequently forces the secret world into proving its "added value" in relation to cost, risk, and time, on every topic, every day.

Emerging Prospects

Apart from increased public access to the Internet—inclusive of electronic mail, the deep web, and the dramatically increased availability of free multimedia communications and information sharing capabilities—several factors are supportive of a displacement of secret sources and methods by open sources and methods:

Digitization

It is a mistake to believe that all relevant information is being digitized today. Tribal histories (e.g., those from Iraq) and vast quantities of important information are still being produced in Industrial Era media, and Friday sermons by Islamic imans, as well as the sermons by all the other faiths, are not part of the digital revolution. In strategic terms, however, digitization is extremely important for three reasons:

1. Most current information from mainstream and niche media as well as individual publishers and bloggers, in all languages, is now available digitally.
2. Historical information, including policy and financial statements of great importance to specific nations, industries, organizations, and tribes can now be affordably and effectively digitized.
3. Hand-held devices are rapidly becoming a primary means of collecting and sharing information, with imminent prospects of being able to harness, selectively, all that any group of individuals can see and hear and think, and is willing to upload as needed.

VISUALIZATION

Digital information, including historical information, can now be visualized, not only in relation to content analysis and links between paragraphs and among individuals, but in relation to a geospatial foundation such as Google Earth provides in rudimentary but quite compelling terms. This is moving OSINT well beyond secret sources and methods because it can draw on a much greater body of information and expertise in real time, and apply all modern machine analytic tools with fewer security, legal, and policy constraints. The centralized, unilateral, secret bureaucracies are losing ground—rapidly—to distributed, open, multinational networks.

PEER-TO-PEER (P2P)

"Ground truth" is taking on a whole new meaning as individuals exercise the power to share complex information directly with one another, eliminating the intermediary journals, web sites, and government or media offices that in the past have played the role of editor, judge, and broker of meaning and value.

The power of OSINT at the strategic level can neither be exaggerated nor underestimated for the simple reason that it harnesses the distributed intelligence of the whole earth, in real time as well as in historical memory time, across all languages and cultures. There is not a bureaucracy in the world that can match its networked power. To drive that point home, consider the game of baseball. In today's secret environment, government bureaucrats accustomed to unlimited budgets and secret methods continue to try to win the game by bribing a player (clandestine intelligence), putting a "bug" in the dugout (signals intelligence), trying to "sniff " the direction and speed of the ball (measurements and signatures intelligence), or taking a satellite picture of the field every three days (imagery intelligence). The new craft of intelligence integrates the audience. It uses the collective wisdom of all the participants. It encourages the crowd to participate. Open source intelligence harnesses what everyone sees and knows. It changes the rules of the game. Any catch in the stands is an out. That is

how we win against asymmetric opponents who know our Achilles' heels all too well.

OSINT AND ELECTORAL REFORM

The United States is a republic. An extraordinary characteristic of republics is that voters have the power to dissolve the government should it become so ineffective or destructive as to warrant its termination. The Constitution, and the voters, are the foundation of the American democracy, not the three branches of government. If the Executive is mendacious, the Congress is corrupt, and the Judiciary is so unrepresentative of the values of the people as to be a mockery of justice, then the public has the power to change the rules of the game for elections. It is OSINT that can be used by citizens to break away from the Republican and Democratic parties, and develop new networked means of demanding minimalist changes such as suggested by Ralph Nader and enhanced by the author: voting on weekends so the poor do not lose work; restoring the League of Women Voters as the arbiters of multiparty debates; demanding that presidential candidates announce their Cabinets in advance of the election, and including at least the Secretaries of Defense and State, and the Attorney General, in Cabinet-level debates; applying the instant runoff concept to ensure a true majority election; and, of course, ending gerrymandering and corporate funding for any elected official.

OSINT AND GOVERNANCE REFORM

Government at the federal level has become incompetent, and is wasteful of the taxpayer dollar for two reasons: special interest corruption both in Congress (bribery) and in the Executive (revolving-door favoritism); and an industrial-era structure that is largely disconnected from reality to the point that ideological fantasy can supplant a reasoned policy process. At a minimum, the republic needs a coalition Cabinet and some means of assuring the citizenry that presidents will not be able to simply appoint cronies from their own party; the Executive needs to be restructured to provide for integrated policy development, not just national security policy development; strategic planning focused out seven generations (over 200 years) must be demanded and be publicly transparent and accountable; and the fundamentals of national power must be mandated: quality education for all, health care for all, and an end to poverty at home. Presidents and their teams must be elected for their ability to govern rather than campaign. OSINT will make all of this possible, sooner than later if a national Open Source Agency is created as a new fourth branch of government, independent of Congress and the Executive, with a lifetime appointment for its Director, and a Board of Directors composed of former presidents, leaders of the Senate and House, and retired Supreme Court justices.

OSINT AND STRATEGIC BUDGETARY REFORM

Finally, we come to budgetary reform. OSINT has already made it clear that we have a Department of Defense costing $500 billion a year (not counting the cost of the war in Iraq) that is relevant to only 10 percent of the threat (state-on-state warfare), that is largely incompetent at small wars and homeland defense, and that we are, as a republic, not investing properly in peaceful preventive measures inclusive of the spread of participatory democracy and moral capitalism. The return on investment on our "big war" military is not only not there, the existence of that big war force leads ignorant presidents and their mendacious vice-presidents to seek out wars as an option for capturing "cheap" oil (never mind the cost in blood, spirit, and treasure). The American republic, specifically, and all other countries are long overdue for what I call "reality-based budgeting." OSINT will restore sanity and sensibility to the public treasury and how it is applied.

There is, in the immortal words of Arnie Donahue[44] in 1992, "plenty of money for OSINT." There is also plenty of money for participatory democracy and moral capitalism. Our problem has been that we have allowed the mandarins of secrecy to pretend to be informing the president, rather narrowly and very expensively, while failing to demand that the republic develop a public intelligence capability suitable for directing public policy and public spending in an intelligent, sustainable manner.

September 11, the Iraq War, and the varied accomplishments—or crimes—of the Bush administration may stand in history as a bright turning point in the history of the republic. One doubts that anything less might have awakened the somnolent public.

NOTES

1. The "seven tribes" is a concept developed by the author and includes government, military, law enforcement, business, academia, the ground-truth tribe (nongovernmental organizations and the media), and the civil-sector tribe (citizen advocacy groups and societies, labor unions, and religions).

2. This term, "Revolution in Intelligence Affairs," is abused by loosely educated individuals who know nothing of revolution and little of all-source intelligence. For a critique of the abuse of the term, and a discussion of the three options for intelligence reform, see the author's "Intelligence Affairs: Evolution, Revolution, or Reactionary Collapse," *International Journal of Intelligence and Counterintelligence* 19 (Spring 2006), pp. 187–189. In a forthcoming issue the author comments on "Intelligence in Denial."

3. This is a practical professional discourse on OSINT, not a political diatribe, but it is essential for those who have the most to gain from OSINT, citizens, to understand that the extremist Republicans have driven out the moderate Republicans (including the author) while the inept Democrats have alienated both the conservative Democrats and the

New Progressives. For an excellent and erudite discussion of why the prevailing mood of the country may well be "a pox on both parties," see Peter Peterson, *Running on Empty: How the Democratic and Republican Parties Are Bankrupting Our Future and What Americans Can Do About It* (New York: Farrar, Straus and Giroux, 2004). Peterson was a Cabinet Secretary under Nixon and Chairman of the Council on Foreign Relations. He joins numerous other moderate Republicans who have published books dismissive of the Republican Party as it has been hijacked by the religious extremists, the neo-conservatives, and corporate war-profiteers. The Democratic leadership is equally corrupt, but so inept as to be incapable of either governing or holding the Republicans accountable.

4. Howard Rheingold, *Smart Mobs: The Next Social Revolution* (New York: Basic Books, 2003); James Surowieki, *The Wisdom of the Crowds* (New York: Anchor, 2005); and Pierre Levy, *Collective Intelligence: Mankind's Emerging World in Cyberspace* (New York: Perseus, 2000). Three other essential references are H. G. Wells, *World Brain* (London: Ayer, 1938); Howard Bloom, *Global Brain: The Evolution of Mass Mind From the Big Bang to the 21st Century* (New York: Wiley, 2001); and Tom Atlee, *The Tao of Democracy: Using Co-Intelligence to Create a World That Works for All* (San Francisco:Writer's Collective, 2003). Robert Steele addresses the concepts and doctrine for actually "doing" collective public intelligence in *The New Craft of Intelligence: Personal, Public, and Political* (Oakton, VA: OSS, 2002).

5. It is now clearly documented that both the White House and the Senate knew that Peak Oil was upon us during varied hearings conducted from 1974–79, and deliberately concealed this fact from the public, and failed to alter energy policy, in order to avoid alarming citizens or angering them over prices, while continuing to reap the rich dividends of bribery from the oil companies. This is a single specific example of where retrospective impeachments would be appropriate as a means of putting all elected officials so that they will be held accountable not just today, but into the future as their treasonous betrayal of the public trust becomes known.

6. There are 20,000 pages on OSINT at http://www.oss.net, and a one-page list of key familiarization links covering history, context, practice, policy, and reference are at http://www.oss.net/BASIC. To this day, the secret intelligence world refers with disdain to OSINT as "Open Sores."

7. The single best book on the cost of the Cold War is Derek Leebaert's *The Fifty-Year Wound: How America's Cold War Victory Has Shaped Our World* (Boston: Back Bay Books, 2003). Chalmers Johnson has written two books in this genre, the first and most recent more methodical than the second: *The Sorrows of Empire: Militarism, Secrecy, and the End of the Republic* (New York: Metropolitan Books, 2004), and *Blowback: The Costs and Consequences of American Empire* (New York: Owl, 2004, reissue). See my partial list of books on blowback at http://tinyurl.com/qrcdu. An entire literature on "why people hate America" has been developing, along with U.S.-based critiques of immoral capitalism and virtual colonialism.

8. General Alfred M. Gray, Commandant of the Marine Corps, "Global Intelligence Challenges in the 1990s," in *American Intelligence Journal* (Winter 1988–89), pp. 37– 41. Despite four years of effort by the Marine Corps, the National Foreign Intelligence Board (NFIB) and the Military Intelligence Board (MIB) refused to address General Gray's recommendations that we change our priorities from worst-case least probable to most probable emerging threats, and that we invest in open sources. Had we done so from 1988 to 2000, in those twelve years we would probably have collected enough open sources in

Arabic and other languages to understand the threat represented by bin Laden in terms compelling enough—because they were public—to mandate sustained effective action by all relevant national capabilities.

9. Daniel Ellsberg, *Secrets: A Memoir of Vietnam and the Pentagon Papers* (London:Viking, 2002). This is his recollection of his words to Henry Kissinger, then National Security Advisor to President Richard Nixon. The three pages on the pathological effects of falling prey to the cult of secrecy, on pages 237–39, should be forced rote memorization for all who receive clearances.

10. General Tony Zinni, U.S.M.C. (Retired), former Commander-in-Chief, U.S. Central Command (CINCCENT), as recounted to the author on April 4, 2006, by a very prominent individual close to varied National Security Council and defense personalities, who desires to remain anonymous.

11. As recounted in Richard Helms, *A Look Over My Shoulder: A Life in the Central Intelligence Agency* (New York: Random House, 2003).

12. Cf. Robert Steele, *On Intelligence: Spies and Secrecy in an Open World* (Fairfax, VA: AFCEA, 2000; Oakton, VA: OSS, 2003) with a Foreword by Senator David Boren (D-OK), whose efforts to reform national intelligence in 1992 were undone by a combination of Senator John Warner (R-VA) and Secretary of Defense Dick Cheney. The book remains the single most comprehensive public critique of the shortfalls of the secret world. For a list of other books critical of the past and offering a vision for the future, see my varied lists at Amazon.com.

13. Cf. Walter Laqueur, *A World of Secrets: The Uses and Limits of Intelligence* (New York: Basic Books, 1985). Many other books give accounts of secret warfare going back in time, but culminating in the behind-the-lines operations in World War II, and then the "dirty tricks" of the 20th century.

14. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press, 1948). This is a classic. In reality, Kent did not achieve his vision for two reasons: because the clandestine service took over the Central Intelligence Agency and subordinated the analysts, and because, in so doing, they cut the analysts off from the world of open sources that were the mainstay of Kent's vision in the first place.

15. Robert Steele is the primary author on the concept of "smart nation." Among the early works were "Creating a Smart Nation: Information Strategy, Virtual Intelligence, and Information Warfare," in contributing eds., *Cyberwar: Security, Strategy, and Conflict in the Information Age,* contributing eds. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (Fairfax, VA: AFCEA, 1996), pp. 77–89; "Creating a Smart Nation: Strategy, Policy, Intelligence, and Information," *Government Information Quarterly* 13 (Summer 1996), pp. 159–173; "Reinventing Intelligence: The Vision and the Strategy," *International Defense & Technologies* (December 1995), bilingual in French and English; and "Private Enterprise Intelligence: Its Potential Contribution to National Security," paper presented to the Canadian Intelligence Community Conference on Intelligence Analysis and Assessment, October 29, 1994, reprinted in *Intelligence and National Security* (Special Issue, October 1995), and also in a book by the same name, 1996.

16. The sections that follow deliberately relate OSINT to reform of the secret elements of the intelligence cycle. Complete multimedia lectures, a total of eight, are easily accessed via http://www.oss.net/BASIC.

17. (New York: United Nations, 2004). The endeavor benefited from the participation of The Honorable Lieutenant General Dr. Brent Scowcroft, U.S.A.F. (Retired),

former national security advisor to President George Bush. Terrorism is ninth out of the ten high-level threats. The report, 262 pages in length, can be seen at http://www.un.org/secureworld/report2.pdf.

18. It merits comment that according to the *Report of the Commission on the National Imagery and Mapping Agency*, as published in December 1999, most of the intelligence money is spent on esoteric collection systems, and almost none at all is spent on actually making sense out of the collected information.

19. The author has served in the clandestine service (six tours, three overseas), supported strategic signals intelligence acquisition operations, and been a member of the Advanced Program and Evaluation Staff (APEG) with responsibilities for national-level validation of current and future secret imagery collection programs.

20. The languages that OSS and its partners use to follow terrorism and other topics properly are as follows: Arabic, Aramaic, Berber, Catelan, Chinese, Danish, Dari, Dutch, English, Farsi, Finnish, French, German, Indonesian, Irish, Italian, Japanese, Korean, Kurdish, Kurmanji, Norwegian, Pashto, Polish, Portuguese, Russian, Serbian, Spanish, Swedish, Tamil, Turkish, and Urdu. Arabic variations include Andalusi Arabic (extinct, but important role in literary history); Egyptian Arabic (Egypt), considered the most widely understood and used "second dialect"; Gulf Arabic (Gulf coast from Kuwait to Oman, and minorities on the other side); Hassaniiya (in Mauritania); Hijazi Arabic; Iraqi Arabic; Levantine Arabic (Syrian, Lebanese, Palestinian, and western Jordanian); Maghreb Arabic (Tunisian, Algerian, Moroccan, and western Libyan); Maltese; Najdi Arabic; Sudanese Arabic (with a dialect continuum into Chad); and Yemeni Arabic.

21. This is a very serious indictment of both the policy community and the intelligence community. It is based on direct observation in three embassies overseas (three tours), on a second graduate thesis on strategic and tactical information management for national security, and on eighteen years of advocacy during which over forty governments have been helped to enhance their access to and exploitation of open sources of information.

22. The author spent a tour in the Collection Requirements and Evaluations Staff (CRES) at the CIA, and also consulting in the 2000–1 timeframe to ICMAP, the attempt by the Deputy Director of Central Intelligence for Administration (DDCI/A) to reduce duplicative tasking of the varied classified collection disciplines. Neither the CIA nor the new Open Source Center have a full grasp of how to access all information in all languages all the time, and ICMAP continues to focus on triage among the classified systems, without regard for what can be found, gotten, or bought.

23. This is the only standard that may not be readily apparent when this chapter is published. Invented by Doug Englebart, also the inventor of the mouse and hypertext, this standard enables linkage of related content to take place at the paragraph level, which also allows copyright compliance to be executed at the paragraph level, for pennies instead of dollars.

24. Amy Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Palo Alto: Stanford University Press, 2000).

25. It is a fact that 90 percent of the information that we need to gain access to is controlled or obtainable by nongovernmental, academic, civil, and generally foreign organizations that cannot afford the gold-plated and generally pathologically dysfunctional information technology systems that the beltway bandits have been selling to the secret world for decades. In order to create a global information sharing environment where we

can get much more than we give in the way of content (what we can provide is processing power), it is essential that we establish generic open source software suites of tools, such as the Defense Advanced Research Projects Agency (DARPA) has done with STRONG ANGEL, so that all relevant contributors can join the Open Source Information System (OSIS) via inexpensive collaborative toolkits and access ports.

26. Information technology has not been an obstacle to the creation of 24/7 "plots" but rather mindsets and bureaucratic inertia. For a stimulating and truly enlightening account of both the early mistakes and later successes of the British in World War II in using "plots" to track and anticipate the movements of submarines (a skill applicable to today's terrorists), see Patrick Beesley, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre, 1939–1945* (London: Greenhill, 2000). As with all books cited, a summative review by Robert Steele, with key points itemized, can be read at Amazon.com.

27. Despite General Gray's concern in 1988, and years of effort by the author that culminated in testimony to the Aspin-Brown Commission resulting in a finding that our access to open sources was "severely deficient" and should be a "top priority" for funding; and despite a report commissioned by DCI George Tenet and delivered by Boyd Sutton in July 1997 on "The Challenge of Global Coverage"—a report recommending that $1.5 billion a year be spent on open sources as an insurance policy, consisting of $10 million a year on each of 150 topics of lower tier countries spawning terrorism, crime, disease, and other ills—Tenet, his predecessors, and his successors have consistently refused to focus on anything other than secrets for the president. The Global Coverage report is easily accessible via http://www.oss.net/BASIC.

28. There are a handful of books that really emphasize the importance of history and the continuing strategy relevance of historical factors including morality and birth control (or not). Among them: Will and Ariel Durant, *The Lessons of History* (New York: Simon & Schuster, 1968); Richard Neustradt and Ernest May, *Thinking in Time: The Uses of History for Decision Makers* (New York: Free Press, 1988); Stewart Brand, *The Clock of the Long Now: Time and Responsibility—The Ideas Behind the World's Slowest Computer* (New York: Basic, 2000); and John Lewis Gaddis, *The Landscape of History: How Historians Map the Past* (New York: Oxford, 2004). Included here are two books on the strategic implications of losing history, and failing to notice fact: Robert Perry, *Lost History: Contras, Cocaine, the Press & "Project Truth"* (San Francisco: Media Consortium, 1999), and Larry Beinhart, *Fog Facts: Searching for Truth in the Land of Spin* (New York: Nation Books, 2005).

29. This term was first used by Alvin Toffler to describe the author, his company, and OSINT. See the chapter on "The Future of the Spy" in which five of the twelve pages are focused on OSINT, in *War and Anti-War: Making Sense of Today's Global Chaos* (New York: Warner, 1995). All of the books by the Tofflers, who now write as a team, are relevant to the information era, but *Powershift: Knowledge, Wealth, and Power at the Edge of the 21st Century* (New York: Bantam, 1991) is rather special.

30. This term (M4IS) was first introduced by the Swedes at the Third Peacekeeping Intelligence Conference held in Stockholm in December 2004. The Swedes have replaced the Canadians as the neutral third party of choice.

31. Googling for "analytic tradecraft" is always useful. The actual notes from Jack Davis can be accessed via http://www.oss.net/BASIC.

32. As with all observations in this chapter, the specifics are easily accessible via http://www.oss.net/BASIC, in this case as "New Rules for the New Craft of Intelligence," under Practice, where other guides to analytic tradecraft may also be found.

33. Cf. Robert Steele, *Information Operations: All Information, All Languages, All the Time* (Oakton, VA: OSS, 2006) and—more focused on the military as well as free—*Information Operations: Putting the I Back Into DIME* (Strategic Studies Institute, February 2006). The latter is easily found by Googling for the title.

34. Jonathan Schell, *The Unconquerable World: Power, Nonviolence, and the Will of the People* (New York: Owl, 2004).

35. The author spent a tour at the national level responsible for offensive counterintelligence against a denied area county, and was also responsible for global oversight of recruitment efforts against all representatives of the same government.

36. In general the reader is referred to the 770+ books reviewed by the author at Amazon.com over the past five years. Dr. Colonel Max Manwaring (Retired) has edited *Environmental Security and Global Stability: Problems and Responses* (Lanham, MD: Lexington, 2002) and there is an entire literature on ecological economics as well as on the health of nations, relating disease, poverty, and the environment.

37. On this vital topic, see on the internal threat, two books: Kevin Philips, *American Theocracy: The Peril and Politics of Radical Religion, Oil, and Borrowed Money in the 21st Century* (New York: Viking, 2006), and Michael Lerner, *The Left Hand of God: Taking Back Our Country From the Religious Right* (New York: Harpers, 2006). On the external threat, though there are numerous books on radical Islam, the best overall discussion of ideology as a means of changing the pecking order among social groups, and grabbing real estate and resources, is offered by Howard Bloom, *The Lucifer Principle: A Scientific Expedition Into the Forces of History* (Boston: Atlantic Monthly, 1997). The book includes a prescient discussion of Sunni versus Shiite, as well as of religion as an ideology used to capture resources.

38. Among the most obvious and hard-hitting current references on immoral capitalism are Clyde Prestowitz, *Rogue Nation: American Unilateralism and the Failure of Good Intentions* (New York: Basic, 2004); John Perkins, *Confessions of an Economic Hit Man* (New York: Plume, 2005); William Greider, *The Soul of Capitalism: Opening Paths to a Moral Economy* (New York: Simon & Schuster, 2004); and, most recently, Jeffrey Sachs, *The End of Poverty: Economic Possibilities for Our Time* (New York: Penguin, 2006). There is a separate literature on "virtual colonialism" and the inner anger that a U.S. military presence inspires, particularly in Muslim countries.

39. *Report of the Commission on Protecting and Reducing Government Secrecy* (GAO, 1997), available at http://www.fas.org/sgp/library/moynihan/.

40. Both are available online.

41. No disrespect is intended in neglecting to address the standard works on strategic warning. The author's concept of strategic warning is much broader than now exists within both the secret intelligence world and the academic world that writes about the secret intelligence world.

42. Colin Gray, *Modern Strategy* (New York: Oxford, 1999). An eight-point summary is at Amazon.com. A superb monograph on strategy (eighty-three pages) by Dr. Colonel Harry (Rich) Yarger (Retired), "Strategic Theory for the 21st Century," is easily found online by Googling the author and title.

43. John Perry Barlow, "Why Spy?" *Forbes* (October 7, 2002), available at http://www.forbes.com/asap/2002/1007/042.html.

44. At the time, Donahue was the ranking director with the Office of Management and Budget (OMB) for all Command and Control, Communications, Computing, and Intelligence (C4I), and one of a handful of individuals with all of the code-word clearances. His boss, Don Gessaman, the ranking civil servant at OMB for National Security inclusive of Programs 50 (International Relations) and 150 (Defense), guided the establishment of Code M320 for defense expenditures on OSINT in 2000. OSINT is seen by the intelligence community as a threat that should not be outsourced, and by OMB as a function that can be accomplished in the private sector and therefore should be outsourced to the fullest extent possible.

7

THE SHORTEST DISTANCE BETWEEN TWO POINTS LIES IN RETHINKING THE QUESTION

Intelligence and the Information Age Technology Challenge

DANIEL S. GRESSANG IV

INTELLIGENCE SERVICES, AND THE PRACTICE OF INTELLIGENCE, are at a threshold. The tremendous changes in the global political, economic, security, and technology environments are radically altering not only the mechanics of intelligence production, but the very roles and purposes of intelligence. The collapse of the Soviet Union and the dissolution of the Warsaw Pact forced Western intelligence services to reconceptualize threats and vulnerabilities as they sought to redefine collection and analysis priorities. The Soviets and their allies are no longer the primary target for intelligence. Instead, the new world of the 21st century offers intelligence a wide variety of potential targets, each of which exhibits a host of unique patterns of activity and capabilities. The world has moved from the bipolar moment of the Cold War, through the unipolar moment of little-questioned American supremacy, to the emerging multipolar moment of an emerging Third World and proliferation of nonstate and substate actors on the global stage. The result for intelligence is a complex array of threats, potential threats, and questions, each of which demands understanding and answers, and a formidable set of challenges intelligence will have to overcome to remain vital and relevant to its customers.

Perhaps the most important challenge faced by the U.S. intelligence community stems from the explosive growth in technology. Improvements in telecommunications, computers, and other high-technology fields have ushered in an era of global connectivity and greater interdependence. Information, the root of all intelligence production, has become the principle commodity in this environment. Indeed, the National Intelligence Council's effort to envision the world of 2020 called the growing connectedness of globalization a "mega-trend" that will "substantially shape all the other major trends" of the future.[1] In politics and

governance, technology-driven interconnectedness has fueled the rise of nonstate actors on the world stage, allowing a host of political movements an international status and weight they would not have enjoyed otherwise. In business, technology-driven globalization has broken down trade barriers, allowing both greater flow of goods and services and greater potential for disruption. And in intelligence, it has fostered positive growth and evolution in collection, processing, and analytic capabilities, while also stimulating the capabilities of intelligence collection targets, allowing them new opportunities to prevent or disrupt intelligence collection efforts against themselves. It is, for intelligence, a two-edged sword.

SHIFTING PERSPECTIVES

With the explosive growth in technology and the changes in the international environment, the intelligence community faces very real, and in some ways daunting, challenges. Persistence in conducting the business of intelligence as it always has will quickly prove inadequate, most observers seem to suggest. Gregory Treverton, for example, goes as far as to maintain that "the world as it is now undercuts all the attributes of the old intelligence paradigm, and another decade or more of change would do so even more drastically."[2] Failure to recognize the paradigmatic shift, away from the only one U.S. intelligence has known to an information-dominant one, will result in a diminished capacity for intelligence to serve its core customers of political and military decision makers. As secrets become less and less important and open source information gains greater impact in decision making, the intelligence community must shift focus from state-centric emphasis on secrets to a multifaceted knowledge management approach.

The shift has not been easy, since it engenders a variety of potentially conflicting demands.[3] On the one hand, the intelligence community must overcome technological challenges, deciding in course what is feasible to develop and pursue. Coupled with determinations of technological feasibility are the questions of goals for the community: In what direction does the community need to develop in order to meets its customers' present and future information needs? Both sets of questions, in turn, are wrapped around issues of intent and limitations. There will be, as William Nolte notes, difficult decisions to make concerning the techniques and technologies we may have to leave behind, concerning the risks we are prepared to undertake in pursuit of continued relevance in intelligence production, and in how we choose to envision the future and its needs.[4] In short, one of the most pressing issues for the intelligence community is the way in which it meets the technology challenge of the information age. The way the intelligence community addresses the problems associated with information and technology will ultimately determine the degree to which the community remains an important and relevant contributor in the coming decades.

THE ROLE OF INTELLIGENCE

In some respects, the role of intelligence is quite simple: meet the information needs of its policy-making and war-fighting customers in government. Lieutenant General Michael V. Hayden, U.S.A.F., then-Director of the National Security Agency, outlined the foundational role of intelligence simply and eloquently when he noted that "accurate and timely information about the capabilities, intentions and activities of foreign powers, organizations, or persons and their agents is essential to informed decision making in the areas of national defense and foreign relations."[5] Beyond meeting the immediate information needs of decision makers, however, intelligence must also be forward looking, capable of providing decision makers with an accurate and timely assessment of future threats and possible threats, above and beyond the bounds of the immediate. Intelligence, if it is to fulfill its primary missions, must be able to collaborate within its ranks to produce an understanding of a host of adversaries, from traditional nation-states to emergent substate and nonstate actors.[6]

Indeed, the predictive capacity of the intelligence community is the key to its continued success, because planning and preparation to meet future challenges takes time. Looking to the future, the National Intelligence Council envisions a global landscape that holds both relative certainties and critical uncertainties. Those uncertainties include the spread of new technologies, mainly at the hands of aggressive global businesses, which are expected to result in challenges to governance brought about by greater connectivity and information flow. Though the United States is seen as capable of maintaining its leading position in the economic, technological, and military spheres, emerging nations such as China, India, and Brazil are increasingly capable in technological development, leading to more frequent challenges to U.S. leadership.[7] Meeting those challenges requires a refocused intelligence community, albeit one already in the process of changing. By envisioning an intelligence community transforming to "stay ahead of evolving threats to the United States, exploiting risk while recognizing the impossibility of eliminating it,"[8] the Director of National Intelligence has crafted a series of mission and enterprise objectives designed to keep the intelligence community in a position to "maintain competitive advantages over states and forces that threaten the security of our nation."[9] The key to fulfilling that objective lies in evolving from collection-centric intelligence production to information and knowledge management–driven intelligence production.

Knowledge management, the ability to produce relevant information in context in an appropriate and usable form easily accessible to recipients,[10] is the means by which the intelligence community of the 21st century will remain relevant to government decision makers. Knowledge management, and knowledge production, involve much more than just collection. Collection efforts produce data, often raw, unevaluated observations and facts that typically have little meaning to consumers. Data must be massaged, manipulated, and managed

to transform it into information, where it begins to take on the trappings of usable inputs to analysts and decision makers. Information must finally be put into context and usable form, and only then does it become knowledge with lasting relevance and meaning to its recipients.

FINDING DATA: THE IMPACT OF TECHNOLOGY

Finding the data necessary to begin the process of generating knowledge, however, is much easier said than done. Recent advances in technology, particularly communications technology, have meant that the information environment from which data is gathered has exhibited phenomenal growth. The growth of technology means not only that there are more ways to generate information, but that there are also more ways to discover information and more ways to protect and secure information. Technological expansion has been accelerating for a number of years, and can continue to accelerate indefinitely as technological advancements feed off one another and foster new innovations. Technology, then, will become even more of a force multiplier in the information age, available to any and all who have the resources to acquire it and who can grasp the implications of its use.[11]

Forty-five years ago, at the height of the Cold War, for example, communications technology was rather static and predictable in that communications were limited in terms of opportunities and paths of propagation and in terms of available mechanisms for communication. In 1960, for example, there were no facsimile machines and no cell phones, each being at best only an idea. In the 1990s the number of cell phones available and in use rose from 16 million to over 741 million, with an estimated 50,000 new subscribers daily, and by 2000 there were an estimated 14 million facsimile machines in use. Even in the more limited arena of landline telephony, some 630,000 new telephone lines are installed each year, with a growing investment in, and use of, high-capacity fiber-optic lines, one strand of which can carry an equivalent capacity of all existing communications satellites. Investment in fiber-optic cable by the telecommunications industry alone is estimated at $1 trillion or more. Communications traffic on all these systems is reflected in the explosive growth in availability. By one estimate international commercial telephony alone amounted to over 100 billion minutes in 2000, up from 38 billion minutes just ten years earlier. Other estimates suggest there are approximately 35 million voicemail messages left each hour, and the growing use of Voice-over-Internet Protocol (VoIP, in which telephone calls are made using computers) led to the laying of enough fiber-optic cable to transmit the equivalent of one complete Library of Congress every 14 to 15 seconds. Further complicating the picture, the 1990s saw packetized communications, which make computer-to-computer communications over the Internet functional and is widely used in telephony, overtake traditional nonpacketized communications.[12]

The growth and availability of computers mirrors that of telephony yet carries with it even greater implications for intelligence. In 1960 there were roughly 5,000 stand-alone computers worldwide and twenty years later there were still relatively few personal computers in use. By 2000, however, there were estimated to be over 180 million computers in use, most of which are connected to the Internet, with the number of Internet users growing from 4 million in 1990 to over 361 million ten years later. Beyond standard telephone, Digital Subscriber Line (DSL), or cable connections, there are about 100,000 Wireless Fidelity (WiFi) hotspots publicly available, with Europe and North America beginning to catch up to Asia and the Pacific region in availability. In all, some 37 million people log on to the Internet each day, generating 5 million e-mail messages every minute, or some 610 billion messages in 2000 alone, and creating enough digitized content to equal 40 Libraries of Congress. Those same users also generate an estimated 530 billion instant messages a day, with total Internet traffic doubling every 100 days. In static web content alone there were 2.1 billion pages on the Internet in 2000, with 4.2 billion projected by the end of 2001.[13]

The volume of available information is almost incomprehensible, and it continues to grow exponentially. In 2000 the University of California, Berkeley, estimated that all the information created that year totaled 2 exabytes of data, with 1 exabyte equal to 10^{18} bytes. To place that in context, one computer data storage manufacturer estimated that all spoken human communication, since the dawn of time, equaled 5 exabytes.[14] The intelligence community must effectively sift through this vast amount of data to find those bits which are, or have the potential to be, relevant to its customers.[15]

The explosive growth in technology, of which communications and computer technologies are but a part, holds even greater implications for the intelligence community than sheer numbers alone suggest. Fast-growing and dispersing technology empowers those who adopt and apply it, leading to a growing number of state and nonstate actors capable of influencing global politics.[16] Southern Mexico's Zapatistas, for example, emerged from the jungles in January 1994, seized several small villages, and seemed destined to a quick defeat at the hands of the Mexican army. The Zapatistas and their supporters, however, proved adept at leveraging the Internet to gain and rally support from around the world. As a result, the Zapatistas not only survived, but became a relatively potent advocate for Mexico's poor and downtrodden indigenous peoples. In similar fashion, less developed states that adopt emerging technologies not only afford themselves an opportunity to benefit internally through greater command and control capabilities, but also gain the potential for skipping generations of development in ways disproportionate to outlays, investment, and expenditures. By "leapfrogging" stages of development,[17] these states stand to realize significant progress, placing themselves in some respects ahead of developed states. A country such as the Congo, for example, could, with shrewd and intelligent technology investments, effectively shrink its massive size and streamline command and control through effective adoption of satellite- or wireless-based telephony rather than

spending billions of dollars and countless years rebuilding a poorly maintained and sometimes nonexistent terrestrial telephony infrastructure. By skipping generations of development, the Congo would effectively multiply the difficulties encountered by any intelligence service seeking to access and exploit an architecture that transitions rapidly from early 20th century to cutting-edge telephony.

MOVING FROM THE INDUSTRIAL AGE TO THE INFORMATION AGE

Technological advances, as Michael Herman notes, are obscuring boundaries.[18] Internally, they obscure boundaries associated with geographic spread and the necessities of national-level command and control, as the example of the Congo suggests. Internationally, technology is beginning to erase distinctions between the developed and developing worlds, because each is gaining access to the same technologies and proving successful at applying them. Technology is also blurring distinctions, on the global stage, between state and nonstate actors, because technology allows nonstate groups to leverage and benefit from unregulated mass-appeal institutions such as the Internet. But the challenge of evolving into the information age affects not just the global political environment, it affects in fundamental ways the business of intelligence. The challenges for intelligence, which some have labeled a revolution in intelligence affairs, manifest themselves in collection, processing, analysis, and dissemination of intelligence. Not only has technology begun to blur state-to-state distinctions, it dramatically alters the way intelligence must think about its role and its production. Internally to intelligence, technology offers myriad new opportunities to gather and process information for its customers, while also affording intelligence-collection targets greater opportunities to protect information from collection and exploitation. At the same time, the successes enjoyed in intelligence collection carry their own challenges associated with data overload and dissemination.

Technological advances do more than alter the collection process, because the amount of information gathered and the newer means of processing that information help create a significantly greater amount and variety of information available for analysis and dissemination to intelligence customers. Not only is multisensor coordination possible, those advances also allow a much greater volume of direct "sensor-to-shooter" data transmission, making a tremendous volume of raw data immediately available to operational users. To many, these capabilities alone account for some of the most significant capabilities for the intelligence community to maintain and improve.[19]

To some, this revolution in intelligence affairs has been ushered in through technological advances. In this view, technology provides the enabling capabilities necessary to understand and exploit the growing global information network through the development and deployment of sensor-based automated collection systems. Highly developed and finely tuned sensors, available on a

global scale, will, in this vision, afford commanders and decision makers with instantaneous or near-instantaneous situational displays of selected targets. It is a grand vision, with technological growth and application leading almost seamlessly to vast increases in data suitable for analysis and exploitation. "A single surveillance satellite on a 15 minute pass," according to Major General W. J. P. Roberts, "produces enough material to occupy 100 analysts with conventional tools for a week."[20]

Yet inherent in such visions stands the potential for critical loss of context. Placing the lion's share of emphasis on automation could easily contribute to contextual tunnel vision, in which one aspect of intelligence production—the tangible—is overstressed at the expense of the other—the intangible. This duality of intelligence,[21] however, demands equal weight be given to understanding the adversary's intent as well as his physical locations and capabilities. Effective intelligence production requires, as Herman notes, movement beyond the mere recitation of physical manifestations of the adversary to incorporate interpretations of intent. Knowing the adversary's order of battle, unfortunately, says little about his goals and willingness to use the resources at his disposal. Whereas physical manifestations can only allude to, at best, possible intent, the more difficult aspects of intelligence—intent—are often the province of human intelligence (HUMINT) and signals intelligence (SIGINT) collection. Yet both sets of knowledge, the tangible and intangible, are necessary for defense and planning purposes.

Intelligence is about things and about intentions. It is about knowing and understanding as much as possible about actual and potential adversaries and competitors. It is also about self-awareness, about understanding one's own capabilities, strengths, and vulnerabilities so that effective counterexploitation measures can be developed and adopted. In short, intelligence is about knowing the information environment from all angles and achieving superiority of the information space. This information superiority lies at the heart of what in the defense community is referred to as dominant battlespace knowledge and information assurance initiatives, as conceptualized in the Defense Department's *Joint Vision 2010*:

> Improvements in information and systems integration technologies will significantly impact future military operations by providing decision makers with accurate information in a timely manner. Information technology will improve the ability to see, prioritize, assign, and assess information. The fusion of all-source intelligence with the fluid integration of sensors, platforms, command organizations, and logistic support centers will allow a greater number of operational tasks to be accomplished faster. Advances in computer processing, precise global positioning, and telecommunications will provide the capability to determine accurate locations of friendly and enemy forces, as well as to collect, process, and distribute relevant data to thousands of locations.
>
> Forces harnessing the capabilities potentially available from this system of systems will gain dominant battlespace awareness, an interactive "picture" which will yield much more accurate assessments of friendly and enemy operations within the area of interest.[22]

Achieving dominant battlespace, or information space, awareness raises critical questions for intelligence planners. How is information superiority to be gained and maintained? Can automated systems effectively manage and filter the tremendous volume of information available and collected? How is the volume of data collected to be managed and used? The questions are daunting, leading William Nolte to point out that the intelligence community "must simultaneously confront how information, information technology and information or knowledge management change the world around us, while adjusting to those developments internally."[23]

THE CHANGING ROLE OF INTELLIGENCE

During the Cold War, access to information was at times limited by technological shortcomings or adversarial security practices. Dissemination, and to a lesser degree collection, depended at times on relatively slow systems that were, in turn, dependent on sometimes unreliable communications circuits. This led to a degree of planned redundancy in order to increase the odds of providing an uninterrupted flow of intelligence information.[24] Reliance on system stability and robustness remains equally important today, but with a greater reliance on technology than in the past comes a greater potential for unwanted disruption when systems fail. One recent example is a software anomaly in the National Security Agency's (NSA) system that resulted in a communication infrastructure failure lasting three days. In that time, the NSA was unable to forward intelligence data, to communicate internally, and to process data. Correcting the causal factors and restoring system operability took roughly $1.5 million and involved thousands of man-hours.[25] Lieutenant General Hayden, then-Director of the NSA, reminded audiences afterward that the episode highlighted his agency's absolute reliance on technology.

Improvements in network speed, availability, and reliability—the NSA's troubles notwithstanding—allow for the more rapid relay of information from collector to processor, to analyst, to consumer. In other venues, improved and expanded connectivity and data transfer capabilities allow for significant increases in direct sensor-to-shooter systems, affording operational elements near real-time access to data suitable for mission success.[26] Yet instantaneous or near-instantaneous availability of massive quantities of raw data, or even processed data, may turn out to be a mixed blessing.

Rather than providing the needed information in a context valuable to specific customer needs,[27] direct sensor-to-shooter capabilities flood recipients with largely unevaluated data. Without sufficient filters capable of sorting through the mass of data on the basis of some predetermined set of criteria and translating the raw collection into a usable form of information, recipients are forced to divert attention from immediate operational concerns to an effort to interpret the incoming flow. Although there are numerous examples of successes in such systems, this approach

also holds the potential for disaster, as the example of Beirut illustrates. In 1983 Islamic militants bombed the U.S. Marine barracks in Beirut, Lebanon, with catastrophic results. The Long Commission, tasked with examining the incident to determine and disseminate appropriate lessons learned, concluded on-scene commanders were overwhelmed with data—some relevant, some not; some original, some duplicative—which rendered them ineffective in security planning.[29]

More recently, information overload and the lack of information specificity prevented the intelligence community from developing a clear, comprehensive threat picture prior to the September 11, 2001, attacks on New York and Washington:

> With the huge volume of intelligence reporting that was available prior to September 11, there were various threads and pieces of information that, at least in retrospect, were both relevant and significant. The degree to which the Community was or was not able to build on that information to discern the bigger picture successfully is a critical part of the context for the September 11 attacks.[29]

At the same time, technological evolution and increased technology availability holds the potential for hindering collection and exploitation efforts by enabling adversarial states and groups, thus serving to impose limits on U.S. intelligence production efforts. With each passing day, available technology becomes more standardized as developers and manufacturers embrace the logic and marketability of interoperability. As noted by a panel of experts reviewing technology and business practices at the NSA, "today's information technology is a veritable monoculture. There is very little diversity in the underlying technology and therefore security vulnerabilities found in national security systems as compared with other federal systems [*sic*]."[30] This developing monoculture provides America's adversaries with significant advantages in that they are better able to network, gain more widespread access to information, and better protect their own communications and information technology systems from exploitation.[31]

Greater interoperability in communication and information technology systems is evident not only in advances in digital telephony and computers, but also in the more widespread use of more effective transmission methods and encryption technologies in the private and public spheres. Digital communications allow more widespread use of *packetization*—the parsing of communication at or near its point of origin, transmission by multiple paths, and reassembly at or near the ultimate destination—and forces intelligence collectors to focus their own efforts in a much narrower range of potential access locations.[32] Digitization also makes simpler the use of a range of encryption and other security practices designed to boost user security. As publicly available encryption algorithms gain in length and complexity, the already difficult task of breaking newer encryption schemes can be expected to get harder over time.

Open source information availability adds to the problems faced by intelligence, sometimes immeasurably so, by giving collection targets access to a

range of previously unavailable information and, when security fails, insights into the capabilities and operations of intelligence agencies. Leaks of classified information serve as warnings for those targets, frequently leading to behavioral and technology changes designed to reduce or eliminate vulnerabilities available for exploitation. Press reports in 1998 of American interception of Osama bin Laden's cellular telephone communications, for example, led to bin Laden's abandoning the use of cellular phones and increased significantly America's difficulties in locating and capturing him.[33]

The net result of technological advances is a more complex information environment characterized by increased communications and information systems security, faster and more efficient information transmission practices, and exponential growth in information generation and dissemination. The difficulties caused for the intelligence community are especially acute in the technical disciplines such as signals intelligence. Then-Director Hayden succinctly and eloquently summed up those difficulties in noting:

> The volume, variety, and velocity of human communications make our mission more difficult each day. A SIGINT agency has to look like its targets. We have to master whatever technology the target is using. If we don't, we literally don't hear him; or if we do, we cannot turn the "beeps and squeaks" into something intelligible. We have competed successfully against a resource-poor, oligarchic, technologically inferior, and overly bureaucratic nation-state. Now we [have] to keep pace with a global telecommunications revolution, probably the most dramatic revolution to human communications since Gutenberg's invention of moveable type.[34]

It is, as Hayden acknowledged, a revolution that may be accelerating faster than the intelligence community's ability to keep pace. Government research, development, and procurement practices are often given as reasons for the community's relinquished leading role in technology development and deployment. Explosive growth in the information environment has led, over the past twenty years, to a steady deterioration of the community's ability to access desired data when, where, and how desired. Whereas imagery resources have advanced to the point where much of the world is relatively transparent,[35] the paucity of robust, deeply embedded human collection resources remains a target of intelligence reformers and critics.[36] Despite advances in SIGINT collection and processing capabilities, the percentage of available information actually collected and exploited is smaller today than in the past,[37] due in large part to more rapid commercial development and dissemination.

Though the defense and intelligence communities initiated development of many widespread technologies, the country's position as the world's technology leader is declining. Private industry has moved ahead of government to assume a position at the forefront of technological development and implementation,[38] leaving government—and intelligence in particular—in the unenviable role of playing catch-up. Adding to the intelligence community's difficulty in closing the

technology gap with industry are communitywide personnel and resource reductions, often mandated by Congress.[39] The community has, nevertheless, sought to regain much of its lost technological edge by both partnering with private industry and leveraging newer commercial off-the-shelf (COTS) technologies.[40] Yet other factors, such as bureaucratic inertia, resource limitations, and perceptual blinders, limit the community's efforts to overcome the technology challenge.

TRANSFORMATION

In an effort to reverse recent trends, the intelligence community has embarked on a massive effort to transform itself. Many of the organizational and structural changes reach across agency lines, redrawing the community organizational chart to a degree unprecedented since 1947. The technological transformation effort is critical to overall improvement, yet interpretations of the degree of success achieved—and achievable—vary considerably. Some, such as former Director of Central Intelligence Admiral B. R. Inman, note the widening gap between America and the rest of the world in technological development and argue that regaining technological superiority will be possible only with a fundamental shift to private industry leadership. A more optimistic view holds that any future inability to maintain sufficient intelligence production capabilities will not be the result of technological insufficiency.[41] Which of these perspectives will more accurately describe the intelligence community's future is as yet still undetermined. What can be said, however, is that the intelligence community's monopoly on leading-edge technology has been irretrievably broken,[42] forcing the community to rely more on development partnerships and creative leveraging of existing commercial technologies. The intelligence community's targets have seized the advantage, in one respect, in that they are not forced by circumstances to develop unique capabilities; rather, they only need to select, purchase, and use available equipment.[43]

Transformation will not come easy. Efforts to achieve wholesale change in material resource utilization, business practices, organization, and operative perspective are fraught with danger, particularly when change initiatives seek to modify or undo over forty years of institutional inertia. Pressures toward specialization raise the possibility of transforming into an "intelligence boutique" with severe and effectively debilitating limits on production, customer service,[44] and operational flexibility. Resource reductions, particularly funding, increase the likelihood of boutique development as the intelligence community seeks to maximize value by focusing efforts and expertise on a select set of high-value targets. Complex procurement and budget justification practices developed in part to enhance technical superiority and ensure quality control exacerbate this trend,[45] leaving some segments of the community scrambling to reprogram resources.[46]

Technology, in and of itself, however, is not the most pressing problem faced by the intelligence community as it struggles to transition into an effective and efficient information age producer. COTS, and their effective incorporation into

the intelligence production process, coupled with robust and mutually beneficial government-private industry partnerships, will likely allow intelligence to keep pace with the technological evolution of its targets.[47] A few speed bumps, most likely of short duration, can be expected along the way, but by and large the intelligence community can be expected to have sufficient foresight into technology evolution, and intelligence needs, to effectively combine the two into a coherent program yielding long-term operational sufficiency. The community's technological evolution efforts will need to remain dynamic and wide-ranging,[48] and whereas research and development efforts are well positioned to meet the technology challenge, static and burdensome bureaucracies characteristic of the community add a slight damper to the transformation effort.[49] The NSA's New Enterprise Team (NETeam), tasked by then-Director Hayden to examine the Agency and its practices to recommend improvements, was rather blunt in noting: "Absent profound change at NSA, the nation will lose a powerful weapon in its arsenal. Stakeholders and customers are resigned to accept diminished NSA capability, not because of insurmountable technological challenges, but because NSA has proven to be a poor steward of the nation's SIGINT and INFOSEC [information security] capabilities."[50] Though systems development capabilities are sufficient to address the technology challenges, oversight and management of the process demand improvements in strategic focus and leadership.[51] Even more pressing, however, is the perspective that informs the lack of management and focus. The changing information environment—the environment in which intelligence technologies and requirements exist—offers a much greater challenge. As Nolte sees it, the problem centers on the inherent adaptability of intelligence:

> The Intelligence Community's response to the information or knowledge management challenges to its internal practices has been almost reduced to three elements: speed, volume, and connectivity. How do we deal with the enormous increase in the amount of information available to us, to our clients, and to our adversaries? How do we meet the information needs of users increasingly demanding support "within the decision cycle" of their immediate and potential adversary?[52]

The information revolution demands a change in practices and in thinking more than it demands a change in technological capabilities. It demands, as Nolte suggests, a change in our understanding of how intelligence is being fundamentally altered by the realities of technological and political evolution. It demands, in short, a change in paradigm.

REINVENTING THE INTELLIGENCE WHEEL

Paradigmatic change is always difficult, for it engenders a wholesale reevaluation and adjustment of core understandings and beliefs. It is dramatic in its

scope and impact. To many, it is unsettling. Yet one who has embraced such a drastic change is Gregory Treverton, who offers a compelling vision of the future of intelligence. Arguing that the intelligence community is structured, and functions, in a way poorly suited to the needs of intelligence consumers in the information age because of purposive centralization, Treverton sees an intelligence community unduly focused on obtaining secrets, with intelligence production and dissemination dictated more by intelligence agencies than by intelligence customers. In the information age, he asserts, secrets are "transitory" and intelligence's greatest value lies in the effective location, processing, packaging, and distribution of largely open source information. It is, he argues, a world in which effective information marketing, of secret and open sources, defines effective intelligence production.[53]

For intelligence to effectively meet the challenges of technology, a shift in paradigm much like Treverton's is necessary, although perhaps not to the same degree. Mere changes in technological capabilities, bureaucratic structure and organization, or business practices offer minor substantive change and do little more than fix intelligence firmly in an operational rut. None of these transformational efforts address the core perceptual needs of effective intelligence production because all are narrowly focused on tangible and explicit manifestations of support structures and practices. The information age, in contrast, is one that requires continual growth, flexibility, and adaptation. In the fluid information environment continued intelligence value will not come from newer and better collection and processing systems, as Nagy asserts,[54] nor will it come from simply reorganizing the intelligence bureaucracy.[55] Whereas future success needs technical innovation, the more lasting and important change will come only to the extent that the community understands and accepts the need to re-envision information, improve data management and data mining capabilities, and redefine its central mission. Nolte perceptively notes: "The first condition we must, therefore, impose on finding our place in the new information environment is to control the tendency to see our needs and our mission as fundamentally exceptional. The corollary is that we must be precise in determining the areas in which those needs and missions do impose unique requirements."[56]

At the same time, the intelligence community needs to take to heart the House Permanent Select Committee on Intelligence's (HPSCI) admonition that perspectives need to change from that of a passive gatherer of information to that of a proactive hunter.[57] While HPSCI specifically addressed the NSA in that critique, the need to shift perspective away from the target and refocus on the customer's information needs is equally applicable to the rest of the intelligence community. Whereas the industrial age offered fairly static, rigidly organized, and behaviorally predictable targets for intelligence collection, the information age is awash with an ever-shifting milieu of actual, potential, and possible targets with little predictability and even less permanent structure. Satisfying customer intelligence needs in that environment means elevating the specifics of the information need

to prominence, then determining when, where, and how the best opportunities for gathering the necessary data might be found and exploited. Knowledge management—not at the end point of shifting through collected data, but across the spectrum from initial customer questions to final intelligence product and performance evaluation—is the key to overcoming the technical challenges offered by the present and future.

Simply stated, gone are the days when the intelligence community enjoyed superiority in technical capability and access that, when combined, gave the community the ability to elevate target and collection to prominence. In that rapidly fading world, superiority meant that intelligence agencies could apply the entire spectrum of collection resources against a given target, cast a wide and indiscriminate net for gathering data, then sift through the collection take for those bits and pieces of data that met articulated intelligence requirements. Intelligence collected and processed in this way generally met customer needs when the targets were simpler, more rigidly structured and organized, and technically less sophisticated. U.S. intelligence technical superiority allowed for the large-scale gathering of data against a multitude of targets, leaving analysis to become in some respects little more than the "marketing of collection."[58] Collection, and collection capabilities, drove intelligence operations, with intelligence reporting reflecting more collection priorities and operations than customer needs. Collection capabilities far out-stripped processing and analysis capabilities, leaving a significant portion of the decision making in intelligence to collection managers. Analysis was consequently left not as the driver of intelligence efforts, but the backstage player awaiting the collector's largesse. We produced a lot of hay, to use one telling analogy, and it mattered little because we were good at sifting through it.

The information age, however, fundamentally changes the relationship between collection and analysis. As Director of Central Intelligence Porter Goss noted, in this new era "we need to make tough decisions about which haystacks deserve to be scrutinized for the needles that can hurt us most. And we know in this information age that there are endless haystacks everywhere."[59] Future efficiency and relevance of intelligence, then, lie in a more nuanced, more selective, more focused and appropriate application of collection resources. No longer can collection systems be applied against targets about which they might produce relevant information; instead, likely information-bearing targets, and their vulnerabilities to access, must be more carefully identified in the initial stages of collection strategy development so that the most appropriate collection system(s) can be chosen and thoughtfully applied. Poor results in collection efforts, which were once tolerable given the massive volume of raw intelligence gathered, are no longer acceptable given new limits on resources and access. In the information age such inadequacies also mean failure in efforts to collect and produce timely and relevant intelligence against the highest value targets as well as failure to collect against less well-identified, but potentially important and lucrative targets.

INTO THE FUTURE

To meet the challenges of the information age, few would disagree that the intelligence community must keep pace with technological development. Though certainly not perfect predictors, indicators seem to suggest it can. Changing its perspective, however, is even more important because the way intelligence problems are conceptualized and prosecuted is the ultimate determinant of success. The relationship between collection and analysis has to change in order for the intelligence community to effectively leverage both technologies and opportunities for access available to it. Yet collection will not wither in importance, as some suggest;[60] it will remain vital as the engine that empowers intelligence. Without robust collection capabilities, whether directed against open source or secret information, we surrender the very foundation on which intelligence rests. Information age collection will remain important but will be more driven by specific customer information needs than ever before. The information age forces a reversal of the collection-analysis relationship, placing analysis for the first time as the central driving force that steers collection. The fluidity and rapid growth of the information environment dictates equal parts flexibility and focus in intelligence collection and forces a shift from analyzing what's been collected to analyzing what to collect. The shift is subtle but profound in its impact on intelligence collection and production.

Analyzing what to collect, as a new operative paradigm, brings the analytic and collection disciplines together as never before. The future of intelligence effectiveness requires more than simple cooperation between analysis and collection; it demands a melding of the two into a unitary effort driving both constituent components. The more focused application of collection resources that results increases the potential to gather the most relevant and important data possible against any specified target. Merging collection and analysis, which in many ways engender quite different thought processes, will not be simple, especially where old Cold War perspectives predominate, but the shift is necessary if the community is to fully embrace and exploit information age possibilities.

Effective future intelligence production, built around the perspective of analyzing what to collect, will by definition be customer-defined, -focused, and -driven. Intelligence exists to serve its customers, and the demands of production in an age of greater openness and information availability focus attention on the customer's information and intelligence requirements by highlighting the need to be more selective about target selection, choices in obtaining information access, and collection resource application. There are, as DCI Goss noted, far too many haystacks to search. Information age intelligence needs its customers to define for it the haystacks and the needles they need to understand. Intelligence, in turn, must develop and maintain target knowledge in order to help its customers define and refine requirements and to determine not only the most likely venues through which the most relevant data might be available, but to also determine the best ways to access and exploit target vulnerabilities. Target knowledge, then, includes a thorough understanding of the technologies available to the target, now

and as potential acquisitions for the future, as a way of determining target capabilities. Knowledge of target capabilities, defined by the ways the target has chosen to adopt and implement technology, define for intelligence collectors the operational parameters of the targets as well as the target's ability to secure its information from exploitation.

At the same time, target knowledge has to include order-of-battle information, knowledge of target operational capabilities and behaviors, and target tendencies and predilections. From this, the intelligence collector can gain a better understanding of not only target strengths but, more important, of target weaknesses and vulnerabilities. With the identification of actual and potential target vulnerabilities comes the greater opportunity to select the most appropriate collection resource, that which is most capable of exploiting those identified vulnerabilities, from among the available spectrum of collection systems. Collection resource selection requires such knowledge because the most appropriate resource to use often incorporates both the need to exploit vulnerabilities and the ability to gather the sought-after data. One without the other leads to inefficiency and, in times of crises, intelligence failure. A shift to analyzing what to collect opens windows for exploitation that might, given the size and complexity of the information environment, be otherwise overlooked or closed.

Overcoming the challenge of technology and its evolution requires multiple approaches. The U.S. intelligence community can no longer afford to gather and produce intelligence as it did during the Cold War—relying on its superiority in both technology and access. These are monopolies of the past and will do little to allow effective exploitation in the information age. Although the United States may maintain pace with technological advancement, it will probably never again enjoy the overwhelming dominance it once had. Intelligence production will reflect these shifting dynamics in its need to find and adopt appropriate innovations that will allow it to remain vital, relevant, and timely. Improved business practices and streamlined bureaucracies and agencies will almost certainly enable effective adaptation, as will programs either partnering with private industry for technology development or for leveraging COTS technologies as they emerge. Yet it is paradigmatic change, a change in the way we consider information, as well as both analysis and collection, that will afford the intelligence community the ability to make sense of and exploit the information environment. Shifting from the collection resource-centric analyzing what's collected mindset to the newly emergent information needs-centric analyzing what to collect mindset reorients our thinking at a fundamental level and, in doing so, opens up possibilities for effectively addressing the technological challenges of today and tomorrow.

NOTES

The views and opinions expressed in this chapter are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government.

1. National Intelligence Council, *Mapping the Global Future: Report on the National Intelligence Council's 2020 Project*, NIC-2004-13, December 2004, p. 10, available at http://www.cia.gov/nic/NIC_globaltrend2020.html. Hereafter cited as NIC-2004-13.

2. Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (Cambridge, UK: Cambridge University Press, 2003), p. 220.

3. See William M. Nolte, " 'Information Control Is Dead. What's Next?' The Knowledge Management Challenge for the Intelligence Community in the 21st Century," *Defense Intelligence Journal* 9 (Winter 2000), p. 10.

4. Ibid.

5. Lieutenant General Michael V. Hayden, U.S.A.F., Director, National Security Agency, "Address to Kennedy Political Union of American University, 17 February 2000," available at http://www.nsa.gov/releases/relea00058.pdf. Hereafter cited as Hayden, "Address."

6. Director of National Intelligence, *The National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation* (Washington, DC: Office of the Director of National Intelligence, October 2005), p. 1. Available at http://www.dni.gov/NISOctober2005.pdf. Hereafter cited as *National Intelligence Strategy*.

7. NIC-2004-13, pp. 8, 22.

8. NIC-2004-13, p. 3.

9. *National Intelligence Strategy*, pp. 4–19.

10. Different authors advocate different definitions of knowledge management, but most seem to agree with these core elements. Clinton Brooks, for example, defines knowledge management as "making information available effortlessly, in a useable form, to the people who can apply it in their context, so that it is actionable and, thereby, becomes knowledge. It means getting the right information, to the right people, in the right format, at the right time, so they can derive knowledge, and do their jobs better." Dennis Nagy defines knowledge management as "the ability to sustain the knowledge base and to assemble and communicate only pertinent understanding, uncertainties, relevant facts, and environmental influences to the right commander or decision-maker at the right time to keep it up-to-date in the context of the commander's or decisionmaker's [sic] needs." See Clinton C. Brooks, "Knowledge Management and the Intelligence Community," *Defense Intelligence Journal* 9 (Winter 2000), p. 18, and Dennis M. Nagy, "A Military Intelligence Knowledge Base and Knowledge Management: Cultural Factors," *Defense Intelligence Journal* 9 (Winter 2000), p. 43.

11. See NIC-2004-13, p. 34, for a discussion of technology as a force multiplier in all dimensions of life.

12. See Melanie M. H. Gutjahr, *The Intelligence Archipelago: The Community's Struggle to Reform in the Globalized Era* (Washington, DC: Joint Military Intelligence College, 2005), pp. 114–18; Hayden, "Address"; and Lieutenant General Michael V. Hayden, "Statement for the Record by Lieutenant General Michael V. Hayden, USAF, Director, National Security Agency/Central Security Service Before the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, 17 October 2002," p. 6, available at http://www.nsa.gov/releases/relea00064.pdf. Hereafter cited as Hayden, "Statement for the Record."

13. See Hayden, "Address"; Gutjahr, *Intelligence Archipelago*, pp. 114–18; Michael A. Wertheimer, "Crippling Innovation—and Intelligence," *Washington Post*, July 21, 2004, p. A19; and Hayden, "Statement for the Record."

14. Russ Mitchell, "The Ghosts in the Machine: Can Technology Find Terrorists?" *American Spectator* (November/December 2001), cited in Gutjahr, *Intelligence Archipelago*, pp. 114–15.

15. The National Security Agency, to cite but one example, is said to be falling behind in investments needed to maintain pace with technological growth, according to former Director Hayden. See Hayden, "Address."

16. NIC-2004-13, pp. 34–35 and 75–77.

17. NIC-2004-13, p. 10, 12, and 35. See also Gutjahr, *Intelligence Archipelago*, pp. 115–16.

18. Michael Herman, *Intelligence Services in the Information Age: Theory and Practice* (London: Frank Cass, 2001), p. 52.

19. See, for example, Admiral W. A. Owens, "Intelligence in the 21st Century," *Defense Intelligence Journal* 7 (Spring 1998), p. 28, and Herman, *Intelligence Services,* p. 52.

20. Major General W. J. P. Roberts, "Implications of Information Age Operations," *RUSI Journal* 142 (October 1997), p. 39, quoted in Herman, *Intelligence Services,* p. 53.

21. Herman, *Intelligence Services,* pp. 54–61.

22. Joint Chiefs of Staff, *Joint Vision 2010*, available at http://www.dtic.mil/jv2010/jvpub.htm. See also Nagy, "Military Intelligence," p. 40.

23. Nolte, "Information Control," p. 10. For a more detailed walk through the myriad questions that must be addressed on a daily basis, see Hayden, "Statement for the Record," pp. 4–5.

24. Gutjahr, *Intelligence Archipelago,* pp. 119–20.

25. Hayden, "Address," p. 2.

26. Dennis N. DuBois, "Intelligence Community Information Technology: Driving Architecture to Budget," *Defense Intelligence Journal* 9 (Winter 2000), p. 59.

27. Brooks, "Knowledge Management," p. 17.

28. See Department of Defense, "Report of the DoD Commission on Beirut International Airport Terrorist Attack, October 23, 1983," also known as the Long Commission Report, especially Part Four—Intelligence, pp. 57–66. The report is available at http://www.ibiblio.org/hyperwar/AMH/xx/Mideast/Lebanon-1982-1984/DOD-Report/index.html. See also Nagy, "Military Intelligence," p. 43.

29. U.S. Congress, Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001, by the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, p. 7. Available at http://www.fas.org/irp/congress/2002_rpt/911rept.pdf.

30. National Security Agency, "External Team Report: A Management Review for the Director, NSA," October 22, 1999. Available at http://www.nsa.gov/releases/relea00056.pdf.

31. Central Intelligence Agency, *Global Trends 2015: A Dialogue About the Future With a Nongovernment Expert*, NIC-2000-02, December 2000. Available at http://www.cia.gov/cia/reports/globaltrends2015/index.html.

32. M. C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon* (Washington, DC: National Defense University Press, 1995), pp. 140–41. See also Herman, *Intelligence Services,* p. 58.

33. Hayden, "Statement for the Record," p. 2.

34. Ibid, pp. 5–6.

35. See Treverton, *Reshaping National Intelligence*, pp. 217–22, for an interesting discussion of the impact of these changes.

36. See, for example, National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton, 2005), especially pp. 350–52.

37. Hayden, "Address," pp. 5–6, and Hayden, "Statement for the Record," p. 2.

38. Admiral B. R. Inman and Daniel F. Burton Jr., "Technology and U.S. National Security," pp. 117–35, in *Rethinking America's Security: Beyond Cold War to New World Order,* eds. Graham Allison and Gregory F. Treverton (New York: W.W. Norton, 1992), pp. 118–23.

39. As an example, in the 1990s, when telecommunications and information technologies saw some of its most explosive growth, the NSA reduced both its manpower and budget by roughly one-third. Gutjahr, *Intelligence Archipelago,* pp. 116–17.

40. Hayden, "Statement for the Record," pp. 7–8.

41. See Inman and Burton, "Technology," p. 126, and Nagy, "Military Intelligence," p. 41.

42. Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence in the Information Age* (New Haven, CT: Yale University Press, 2000), p. 43.

43. See Hayden, "Statement for the Record," pp. 6–7, and Michael Hirsh, "The NSA's Overt Problem," *Washington Post*, January 1, 2006, p. B4.

44. Hayden, "Statement for the Record," p. 6.

45. Inman and Burton, "Technology," p. 124.

46. The NSA, for example, reprogrammed funds from still-productive programs to emerging technologies development and procurement. Despite reprogramming roughly $200 million, the NSA found the amount far below present and future needs. See Hayden, "Statement for the Record," p. 6. By the same token, the NSA's effort to better the SIGINT production process, called Trailblazer, reportedly has consumed over $1 billion while producing less-than-desired outcomes. See Hayden, "Statement for the Record," pp. 7–8, and Siobhan Gorman, "System Error," *Baltimore Sun*, January 29, 2006, p. 1A+.

47. For extensive discussions of this, see Brooks, "Knowledge Management," especially p. 18, as well as Nagy, "Military Intelligence"; Hayden, "Statement for the Record"; Berkowitz and Goodman, *Best Truth*; and Inman and Burton, "Technology."

48. Nagy, "Military Intelligence," p. 42.

49. See Berkowitz and Goodman, *Best Truth*, pp. 45 and 67–73.

50. National Security Agency, "New Enterprise Team (NETeam) Recommendations: A Management Review for the Director, NSA," October 22, 1999, p. 1. Available at http://www.nsa.gov/releases/ relea00056.pdf. Hereafter cited as NETeam Recommendations.

51. Ibid.

52. Nolte, "Information Control," p. 11.

53. Treverton, *Reshaping National Intelligence*, pp. 217–26. Berkowitz and Goodman take a similar approach in advocating virtual intelligence teams, created on an ad hoc basis to focus on specific questions and needs. See Berkowitz and Goodman, *Best Truth*, pp. 78–83.

54. Nagy, "Military Intelligence," pp. 41–42.

55. For an extensive discussion of the importance of, and need for, new systems development, see for example U.S. Congress, Report of the United States Senate Select

Committee on Intelligence and the U.S. House Permanent Select Committee on Intelligence, Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, S. Rept. No. 107-351, H. Rept. No. 107-792, 107th Congress, 2nd session, December 2002, especially "Technology Gaps," pp. 368–72; "Technical Collection of Terrorist Communications," pp. 373–85; and "Human Intelligence (HUMINT) Collection," pp. 385–92; or the much shorter U.S. House, Permanent Select Committee on Intelligence, Subcommittee on Terrorism and Homeland Security, "Counterterrorism Intelligence Capabilities and Performance Prior to 9-11, A Report to the Speaker of the House of Representatives and the Minority Leader," July 2002, available at http://www.news.findlaw.com/hdocs/docs/terrorism/hsint/71702thsrpt.pdf. Hereafter cited as U.S. House, "Counterterrorism Intelligence Capabilities."

56. Nolte, "Information Control," p. 9.

57. U.S. House, "Counterterrorism Intelligence Capabilities," p. v.

58. Nolte, "Information Control," p. 12.

59. Porter J. Goss, "Global Intelligence Challenges 2005: Meeting Long-term Challenges With Long-term Strategy. Testimony of the Director of Central Intelligence Porter J. Goss Before the Senate Select Committee on Intelligence, 16 February 2005 (as prepared for delivery)," available at http://www.cia.gov/cia/public_affairs/speeches/2004/Goss_testimony_02162005.html.

60. See, for example, Treverton, *Reshaping National Intelligence*, pp. 226–27.

8

INTELLIGENCE ANALYSTS AND POLICY MAKERS

Benefits and Dangers of Tensions in the Relationship

JACK DAVIS

THIS CHAPTER IS OCCASIONED BY PUBLIC INTEREST in reported tensions between Central Intelligence Agency (CIA) analysts and policy-making officials of the administration of President George W. Bush regarding the significance of ties between the Saddam Hussein regime and Al Qaeda terrorists, an important factor in the U.S. decision to invade Iraq in 2003. No evaluation of the latter case is provided. The chapter addresses, instead, general patterns of tensions between intelligence analysts and policy officials, in order to provide a context for public assessment of the Iraq-Al Qaeda incident when the public record is more complete as well as provide enhanced understanding of similar future instances of tension.

Over the years, most of the tens of thousands of written and oral assessments produced by CIA analysts in an effort to support the policy-making process have been received by policy officials with either appreciation or silence. Many of the assesssments are in response to policy-maker tasking, usually a sign of expectation of useful insights. Many consist of briefings and exchanges via telephone or teleconferencing, where the fact that policy officials invest the time to elicit and discuss analysts' assessment of an important national security issue is testimony to the value the officials expect to receive. Many assessments, as to be expected considering the volume of production, miss the mark for the targetted officials in terms of relevancy, timing, or fresh insights, and thus evoke no reaction.

That said, tensions in the relationship between CIA intelligence analysts and administration policy makers are a common occurrence—an essentially normal by-product of the two camps' distinctive professional missions. The analyst's professional commitment is to assess national security issues without bias for or against the outcomes sought by the incumbent presidential administration; the

policy maker's professional commitment is to articulate, advocate, and advance the administration's national security agenda.

Often, the resultant tension in the relationship helps both camps to deal more effectively with the challenges of analytic and policy-making uncertainty that usually attend complex national security issues. Under policy-maker criticism or questioning of judgments, analysts tend to revisit their initial views of the soundness of assumptions about what drives the issue and the implications of incomplete, ambiguous, and contradictory evidence. In response, policy officials often are moved to recalculate the elements of their own assessments of threats to and opportunities for advancing U.S. interests.

At times, though, tensions take a turn that does not serve well sound analysis, effective policy making, or the national interest; charges of *politicization*, or analytic distortion to support or undermine a policy initiative, issue forth from one or both camps. These cases usually arise when policy officials repeatedly reject the analysts' studied interpretative judgments on the status of or outlook for a complex national security issue, especially when such judgments are seen to complicate policy initiatives that are politically important to an administration.

If tensions are a normal occurrence, and their elimination both impractical and unwise, recommendations of ground rules to enhance benefits and curb dangers would seem called for. But first one should make a closer assessment of the roots and branches of the tensions.

Tensions in analyst–policy maker relations in the United States can be traced back at least to the establishment in 1941, under the auspices of the Office of Strategic Services (OSS), of the first bureaucratically independent cadre of intelligence analysts. Sherman Kent, who later played a major role in setting professional standards for CIA analysis, came away from his World War II experience in the OSS with the conviction that relations between producers and consumers of intelligence assessments are not naturally harmonious, despite the common goal of advancing U.S. national security interests. Kent did not much change his views about inherent strains in the relationship during his years of analytic service with the CIA (1951–67).

Why not harmonious? The character of the policy issue at stake, personalities in both camps, the degree of contention about policy direction among administration leaders, and the role of Congress as a third party to the policy-making process from time to time have contributed to the onset and intensity of analyst–policy maker tensions. The underlying constant, though, is the aforemenioned difference in perspective on professsional mission between the producers of intelligence analysis and their policy-making clients.

THE ANALYST'S PERSPECTIVE

CIA analysts are concentrated in the Directorate of Intelligence (DI), which takes pride in its organizational independence from the President, the Secretaries

of State and Defense, and the other policy makers its intelligence assessments are intended to serve. The conceit that DI assessments are free of policy and political influence or bias comes across in the slogans by which the analysts and their leaders usually define their professional mission: *objective analysis*, *carrying truth to power, telling it like it is*.

Over the decades, on many critical and controversial national security issues—for example, Soviet strategic arms, the Vietnam War, Central American insurgencies—considerable substantive expertise, much sweat equity, and tough-minded assessment of assumptions and evidence have gone into the analysts' interpretation of past and ongoing events. The usual bureaucratic result was and is a readiness among analysts to defend key judgments against criticism, even though they are aware of gaps and other flaws in their information.

Regarding prediction of future developments, where unexpected intermediate events can throw seemingly sound forecasts off course, analysts also have confidence in their expertise and work ethic, and they take pride in their belief in the independence of their judgments from policy and political influences.

Concerted public criticism of flawed analytic performance on major national security issues spawns intervals of analytic humility for the DI as an organization, its leaders, and usually the analysts directly involved. But for the most part, confidence, even overconfidence, in substantive judgments is a staple of the analyst's environment. Especially the more experienced DI analysts tend to see themselves as the best informed on the issues they follow as well as the most objective national security professionals in the U.S. government. Over the decades, on many issues they probably have been.

Analysts vary in their experiences with and attitudes toward policy officials. That said, a common first reaction to criticism of their assessments by policy officials is to suspect that either politics or the critics' lack of requisite substantive expertise is at work. Digging in at the heels in defense of the original assessment at times follows. Probably more often, the analysts undertake a reappraisal of their assumptions, evidence, and argumentation, though a substantial change in judgments does not necessarily result.

THE POLICY MAKER'S PERSPECTIVE

Policy officials, for their part, also vary in their experiences with and attitudes toward CIA analysts. A good number of career policy officials over the decades have considered the DI analysts on their accounts not only the best informed among the governmental community of intelligence analysts, but also the quickest to respond to requests for analytic assistance. This subset of policy officials also appreciates that CIA assessments, unlike those issued by analysts in policy-making departments, are rarely skewed to support a party to the bureaucratic politics that usually colors the policy-analysis process on national security issues.

The tendency among officials closest to the president runs differently. These essentially political appointees, because of their own partisan cast, can be quick to attribute partisan motivation to CIA analysts. Especially when a political party has been out of power for some years, newly appointed Republican officials tend to see the Agency as dominated by holdover liberal Democrats, whereas new Democratic officials tend to see the strong influence of Republican conservatives. Many top-level appointees have served in previous presidential administrations and have requisite confidence in their own analytic skills and substantive knowledge of the issues. Some carry over from previous service critical views of the competence of Agency analysts as well as of their perceived propensity to an anti-administration bias.

Regarding professional mission, both career officials and political appointees see themselves as action officers as well as policy analysts. Their job is to get accomplished their vision of the president's national security agenda—the goals, strategies, and tactics that emerge from policy analysis.

Unlike intelligence professionals, policy officials are little pained by a merger of an administration's interests in domestic U.S. politics and foreign policy goals. As a rule, to policy officials, especially presidential appointees, government is politics as well as policy. The merger of policy and political advocacy at times requires building a "yes case" or a "no case" amidst inconclusive evidence of the soundness of a policy initiative and the uncertain implications for policy success of daily developments involving, for example, U.S. diplomatic or military campaigns.

This does not mean administration officials are ready to ignore CIA assessments that, say, would give political opponents in Congress ammunition to criticize policy. Often policy officials will ask analysts to "unpack" their assessment, revealing what is fact and what is opinion, or they will call for a briefing and an exchange of views either to enlighten or to leverage analysts.

In sum, at root, tensions, when they occur, represent a collision between the analyst's mission-driven belief that policy-maker criticism of carefully crafted assesments reflects politics or limited substantive command of issues and the policy official's mission-driven belief that CIA assessments that complicate a well-deliberated initiative reflect antiadministration bias or poor analysis.

THE ANALYTIC BRANCHES OF TENSION: OPINIONS, FACTS, EVIDENCE

Though difficult to untangle in actual cases of analyst–policy maker tensions, separating the varieties of analytic production into three branches—opinions, facts, and evidence—serves to clarify both the character of strains in the relationship and potential ground rules for managing tensions.

Regarding estimative judgments or opinions on issues of high uncertainty (for example, multiyear projections of political developments in unstable foreign

countries, or prediction of the outcome of protracted U.S. military and diplomatic engagements in violence-prone regions), even well-informed policy makers at times gain insights from intelligence analysts' well-argued estimative judgments.

But when analysts' bottom-line judgments are seen as implicit criticism of and potentially harmful to policy agendas, administration officials are prone to dismiss them as "opinions."

Secretary of Defense Donald Rumsfeld, in an October 24, 2002, press briefing, went to great lengths to define the limits of the analysts' opinions in such circumstances: "If you think about it, what comes out of intelligence is not fixed, firm conclusions. What comes out are a speculation, an analysis, probabilities, possibilities, estimates. Best guesses."[1] Further, policy officials claim, often with justification, that the opinions regarding future developments spawned by policy analysis are sounder than analysts' opinions, if only because they are able to take fuller account of the weight of carrots and sticks the United States may be ready to deploy.

More than once, policy officials have let it be known, in particular, that they are little interested in whether analysts think U.S. initiatives will succeed. The analyst's main job, according to critics, is to provide assesssments that enable policy analysts to reach sound judgments about what actions to take to implement policy, despite the uncertainty that fogs complex world events. The analyst's focus should be on strengths and weaknesses of foreign players, their tendencies, motivations, and risk calculations that would help policy officials identify potential dangers and U.S. leverage points.

Regarding facts, tensions are infrequent and usually involve competing methods of determining facts. Here a fact is defined as something concrete and reliably detected and measured: what a foreign adversary said in a recorded speech or intercepted conversation, as opposed to what he or she meant or actually intends to do.

A prominent official once observed, regarding facts, that policy makers are like surgeons. "They don't last long if they ignore what they see once they cut the patient open."[2]

When policy officials are hesitant to accept as fact a condition or development reported by analysts that could complicate political goals or policy implementation, they tend to challenge the sources and methods the analysts relied on in their determination of facts. During military engagements, for example, military officials have preferred to determine battlefield damage to the enemy as recorded in post-flight reports by U.S. pilots, and to dismiss the analyst's usually more modest calculations of damage that were based on, say, overhead imagery.

The most noteworthy tensions between CIA analysts and policy officials usually are over differences about the meaning of available evidence—that is, differences over what to conclude about something knowable but not conclusively known to either intelligence or policy professionals.

On the issues that give rise to major tensions, first, there are gaps in information because of secrecy and collection limitations. Second, the available

evidence reflects a body of reporting parts of which are of questionable reliability and are contradictory and ambiguous. Concerning, for example, the dispute between CIA analysts and prominent administration officials over Saddam Hussein regime's connection to the U.S. war on terror: What will history show the burden of the evidence to have been regarding the nature of Iraq's prewar ties to Al Qaeda terrorists—a minor or major threat to U.S. interests?

Regarding the meaning of inconclusive evidence, former CIA Director and Cabinet member William Casey (1981–87), in a dispute with analysts over the Soviet role in International terrorism, set forth his standard for keeping a policy-sensitive issue on the table: "Absence of evidence is not evidence of absence."[3] In effect, if a development or relationship is plausible, analysts cannot prove a negative to the satisfaction of officials with minds and agendas of their own.

In disputes with analysts about the meaning of inconclusive evidence, policy makers can insist on raising as well as lowering the bar of proof regarding judgments that could have a negative impact on their agendas. Once, when an analyst averred that reliable evidence had become available that indicated a suspected development that undermined an administration policy initiative was "almost certainly taking place," a policy critic retorted that the analyst "couldn't get a murder-one conviction in an American court with [his] evidence."[4]

THE CRITIC'S CHALLENGES TO DI TRADECRAFT

Policy officials have been generous in spelling out the elements of their criticism of Agency analysis. In doing so, the officials at times were motivated principally to improve the quality of support they receive for the demanding task of policy analysis and implementation. At times, the motivation also included an effort to defang or discredit politcally unhelpful assessments. And at times the objective was to shape an intelligence deliverable into a tool that would lend political support to administration policy.

It is worth noting that policy officials who have been generally complimentary of the analyst's performance as well as those long dissatisfied with performance table similar criticisms.

Part of the analyst–policy maker tension in evaluating evidence reflects a difference in professional attitude toward odds. To an analyst, the judgment that the evidence indicates that a development favorable to U.S. interests is unlikely usually means the odds against the existence or emergence of the development at issue are roughly 4 to 1. Given such odds, the busy analyst as a rule is ready to go forward with his or her assessment and move on to the next assignment.

In contrast to a policy maker with an agenda to advance, the same starting odds of roughly 1 in 5 can make it promising as well as politically necessary to stay on the case. Moreover, on politically important issues the official will not overlook the prospect that the analyst's pessimistic judgment could be off base

because, first, they are insufficiently informed about the current state and potential fluidity of foreign forces at play, and, second, because they do not appreciate the impact on developments of U.S. carrots and sticks, if a policy initiative gathers backing.

The reluctance of critical policy officials to rely on what they see as unhelpful assessments on issues important to an administration goes beyond professionally necessary "positive thinking" on their part. Critics also point out what they see as systemic weaknesses in the analyst's tradecraft (i.e., analytic methodologies).

First, since cognitive bias is pervasive, analysts, like all observers, tend to see more quickly and vividly what they expect to see and, conversely, tend not to see and properly credit information that would undermine their prior judgments. Critics contend that analysts delude themselves if they think they are exempt from this so-called confirmation bias because of their claims to "objectivity."

Critics have made this point over the decades in defending requests that analysts take another look at their interpretation of the evidence regarding the rate of success of the strategic hamlet program in Vietnam (1960s), the seriousness of Soviet plans for winning a nuclear war (1970s), the battlefield successes of U.S.-backed insurgents in Nicaragua (1980s), and after September 11, 2001, the significance of Iraqi-Al Qaeda connections to the war on terror.

The analyst's phrase "we have no evidence that *X* exists" is judged particularly unhelpful by those officials dedicated to either blunting the threat or seizing the policy opportunity in question. The critics note that analysts rarely admit they have no evidence that *X* does not exist. Besides, one critic averred, "policymaking is not [done] in a court of law."[5] A similar criticism is that analysts are too tied to the specific reports that reach their "inbox" and do not take sufficient account of the inherent aggressiveness, ruthlessness, and duplicity of U.S. adversaries.

Policy-making critics also complain that analyst training and incentives place too much emphasis on "straight line, single outcome" analysis on complex and uncertain issues. Critics say this "make the call" approach is both unhelpful to sound decision making and prone to error.

Former Deputy Secretary of Defense Paul Wolfowitz, long a critic of Agency analysts, observed in an interview conducted in 1994 that analysts' assertiveness in the face of uncertainty can turn an Agency assessment on complex issues into a weapon for one policy-making camp to use against another. In contrast, by tabling alternative interpretations, analysts would provide a tool useful to all participants in policy debates and decision making.

Further, the critics aver that, especially when policy stakes are high, analysts should expend much more effort evaluating what they don't know and why they don't know it before issuing estimative judgments downplaying dangers on which policy officials are focused. For example, could gaps in information that lead analysts to discount the likelihood of potentially harmful developments of concern to U.S. officials be caused by denial and deception (D&D) operations, or

inadequate U.S. collection, or flawed assumptions about which pathways and relationships an adversary is pursuing to effect the feared development?

The 1999 report of a commission chaired by the current Secretary of Defense Donald Rumsfeld, after noting past intelligence failures on timely detection of foreign ballistic missile developments, cautioned analysts not to be quick to conclude that absence of evidence indicated absence of vigorous weapons programs by potentially hostile countries. The report, instead, charged analysts with pursuing alternative plausible explanations for "particular gaps in a list of [program] indicators."[6]

In truth, policy officials may prize the analyst who can come quickly to a crisp conclusion on issues surrounded by uncertainty that supports their agenda. But policy officials who see CIA judgments as obstacles to their agenda are themselves quick to connect the make-the-call culture to the analyst's record of analytic failures from the Cuban missile crisis to the Iraqi invasion of Kuwait.

Perhaps most important, according to the critics, it is the duty of responsible policy officials to ask probing questions; to insist on critical review of the evidence; to send analysts back to the drawing board for another look; in effect, to pull any loose thread in an unhelpful intelligence assessment.

Secretary of Defense Rumsfeld in his October 24, 2002, press briefing referred to the importance of engagement and criticism: "to the extent there's no feedback coming from . . . a user of intelligence, then one ought not expect that the level of competence . . . on the part of people supplying the intelligence will be as good . . . as if there's an effective interaction."[7] Granted, political overtones often color these criticisms. But in tradecraft terms they represent reasonable standards for policy officials to levy on analysts charged with providing distinctive value added to U.S. policy-making efforts.

DEFINING PROFESSIONAL AND UNPROFESSIONAL ANALYSIS

The doctrinal basis for a response to criticism by administration officials should reflect definitions of professional and unprofessional standards for intelligence analysts as agents both of the national interest and of the policy-making process. Thus, a definition of analytic professionalism should posit as equally important standards both *objectivity* (defined as tough-minded evaluation of evidence and other sound analytic practices) and *utility* (defined as distinctive data and insights policy officials find useful for managing threats to and opportunities for advancing U.S. interests).

Neither objectivity without utility, nor utility without objectivity, would meet the test of the author's following definition: The mission of intelligence analysts is to apply in-depth substantive expertise, all-source information, and tough-minded tradecraft to produce assessments that provide distinctive value-added to policy clients' efforts to protect and advance U.S. security interests. The

analyst's long-held standard of analytic objectivity has helped to promote an institutional ethic of pursing independence from all biases, including policy and political influences, in making judgments in the face of substantive uncertainty. But studies, including those commissioned by the Agency, indicate that *substantive biases* (experience-based mindsets) are all but essential for effectiveness in an environment of high-volume production and tight deadlines. In such circumstances, the effect on production of an "open mind" is akin to the burden of an "empty mind." In addition, *cognitive biases* (especially seeking confirmation for experience-based assumptions amidst inconclusive evidence) in effect are hardwired mental traits.

Pursuit of the defined mission regarding objectivity, then, comes down to an effort to minimize bias by critical review of the assumptions driving the analyst's mindset and of the adequacy of the available evidence to draw any meaningful judgment, and, if so, the content of the judgment.

Also to fulfill the defined professional mission, analytic deliverables must be seen by policy officials to have utility as they define their professional agenda, which, as previously indicated, is to posit and enact an administration's politically colored policy agenda. The analysts who would produce an assessment with high potential for utility to the policy-making process can no more ignore the political context in which their clients operate than they can ignore where the latter are on their learning curves (e.g., how much background information is needed) and decision-making cycles (e.g., planning stage or implementation stage).

To take account of the politics of policy making is not a license for intelligence professionals, as analysts, to become policy makers, or their speechwriters or spear carriers. But if an analyst is not close enough to the process to feel the political pressures affecting policy making, he or she probably is not close enough to produce professionally crafted deliverables that provide distinctive value added.

Thus, there will always be a danger that analysts, in constructing their written assessments and oral commentary, will introduce a policy or political slant—either deliberately or through disregard of analytic standards. Analysts have done so in the past, and likely will do so from time to time in the future.

A politicized and therefore unprofessional assessment can be defined as an analytic deliverable that reflects either (1) the analyst's motivated effort to skew building-block assumptions, evaluation of the evidence, and bottom-line judgments to support—or oppose—a specific policy, political entity, or general ideology, or (2) a conspicuous disregard for analytic standards that produces unmotivated but similarly distorted outputs that could affect the policy-making process.

From the policy makers' agenda-oriented perspective it makes little difference whether what they see as analytic bias is motivated or unmotivated. One senior official, for example, complained that every assessment that indicated or implied that an administration initiative was flawed constituted analytic policy

making, because it provided ammunition for Congress to oppose funding the initiative.

As long as policy-makers' criticism of the objectivity, soundness, or utility of analysis reflects a legitimate tradecraft concern, they are not necessarily putting pressure on analysts to engage in unprofessional behavior. Policy officials have the license to change the intelligence question in search of insights in addition to those embedded in the analyst's initial assessment, to ask that assumptions and evidence be examined more thoroughly, and to request customized follow-on assessments. That is part of their job description, whether they are seeking fresh insights or analytic support for their established views.

Thus, it is not unprofessional behavior for analysts, on their own or when requested, to provide assessments that set out to make the case for an alternative view to their unit's agreed interpretations of ambiguous evidence of ongoing developments and estimative projections of complex trends. The only professional requirements are that such efforts at, say, devil's advocacy, be clearly labeled and vested with appropriate analytic standards for crafting a challenge to the mainline views on an issue embedded with substantive uncertainty.

Additionally, it is not unprofessional behavior for an analyst, when requested, to address matters clarifying tactical policy options for dealing with specific threats to and opportunities for an established general policy. The key to sound "action" or "implementation" analysis is for the analyst to identify plausible initiatives and evaluate them in cost-benefit terms, and for the policy makers to choose what course to pursue and bear responsibility for their decisions.

Finally, for a manager to tighten tradecraft standards on a politically sensitive policy issue before an analyst's assessment goes forward under a corporate DI seal is not necessarily a signal of unprofessional behavior. Painful to the analyst, yes. Politicization of his assessment, no.

Analysts and their managers and leaders must be vigilant in identifying, deterring, and decrying unprofessional assessments as herein defined; when engaged in analysis, they are and must remain intelligence professionals, not policy or political aides—or critics. If an analytic cadre is to deserve its vaunted organizational independence, it must be ready to hold its ground, in the name of the national interest, against pressures for politicization, no matter the source, the intensity, or the circumstances.

But analysts must also take seriously the "cry wolf" danger of levying charges of politicization whenever their authority to control the key judgments of an assessment is abridged.

More to the point, if ever teamwork must prevail over turf warfare and over the individual analyst's sense of entitlement to determine what "call" to make on a matter of substantive uncertainty, it is when the analytic corps is constructing assessments on politically contentious policy issues. Over the decades, many analysts who have made adjustments to initial assessments that maintained objectivity while enhancing utility have felt the sting of colleagues' unreasonable charges of politicization.

THE ANALYST'S RESPONSE TO POLICY-MAKER CRITICISM: BEST PRACTICES

The challenge for analysts, then, is to turn tensions to professional advantage by maintaining rigorous analytic tradecraft standards while enhancing the utility of their assessments to policy makers. Despite a popular reputation for flawed performance, CIA analysts regularly meet this demanding standard. To turn on its head an observation on policy success and failure attributed to President Kennedy after the 1961 Bay of Pigs debacle: Analytic failures draw a thousand critics; analytic successes are orphans.[8]

Call them "ground rules," call them "best practices," lessons can be learned from both failures and successes, and recommendations made for how analysts should respond to policy-maker criticism. The underlying concept behind the recommendations that follow is that analysts carry the heavier burden of managing tensions in policy-maker relations in a manner that advances the national interest.

The main reason is that the policy-making camp is the more powerful of the two. Policy officials have many alternative sources to Agency analysts for information and insight, including their own staffs and departmental analytic organizations; the academic, research, and business communities; the media and the Internet. In contrast, Agency analysts have no comparable alternative market that would justify the large size of their cadre and high volume of production of assessments. Congress demands and receives a steady stream of oral briefings from Agency analysts but is rarely seen as an equal to administration officials as a client for written assessments.

The central theme of the recommendations is that analysts are professionally required to take the tradecraft elements of policy-maker criticism seriously, no matter how much they may perceive that the politics of policy advocacy also are at play. Analysts, thus, should respond to criticism with a reassessment not only of the argumentation and judgments of the original assessment but also of whether it provided utility or distinctive value for the policy-making community. The goal is to take tradecraft issues off the table, so to speak, in an effort to isolate and then defuse any politically motivated elements of policy-maker criticism.

First, become expert on the policy maker's world. Analysts should commit to learning as much about the U.S. policy-making process and their key policy-making clients as, say, a national security correspondent for a major newspaper or other media outlet is expected to command. Analysts, starting from year one, have to spend quality time analyzing how Washington works, warts and all, even if this slows down the pace of grasping how Baghdad, Beijing, or Buenos Aires work. In particular, analysts should understand their client's role as action officer as well as policy analyst. This investment will enable analysts to role-play the policy clients who have criticized an assessment, not to mortgage analytic integrity but to evaluate tradecraft performance through a different set of eyes.

Second, become accomplished at understanding and managing substantive uncertainty. Analysts are taught and are generally aware that their judgments on

complex issues are based on thoughtful but fallible assumptions that in turn color their evaluation of fragmentary, contradictory, ambiguous, and otherwise inconclusive evidence. They have been cautioned about mindset and confirmation bias. Yet the norm is to rely on these powerful but vulnerable mental processes to get their assessments out under tight deadlines, and with a confident judgment.

Usually the resultant assessment holds up well against both the expectations of policy-making clients and the subsequent course of events. Usually. But what to do when a policy official conveys doubts or outright criticism?

Here, without being too quick to jettison original argumentation and judgment, the analysts should move from passive to active awareness of the limitations of their analytic craft. More active attention to the perils of analysis amidst substantive uncertainty entails taking a more thorough accounting of plausible alternative explanations and outcomes that were discarded or downplayed during the crafting of the assessment that drew criticism.

Casual re-examination of an assessment by its author and production unit to take the measure of alternatives at times is helpful, but the process of "talking about alternatives" is prone toward defense rather than critical evaluation of the original argumentation. More structured and externalized challenges to the assessment hold greater promise of fresh insights that either strengthen confidence in, or point to useful modifications of, the assessment that drew criticism.

Tested approaches to alternative or challenge analysis include devil's advocacy, key assumptions check, quality of information review, and argument mapping. A more experimental technique, known as analysis of competing hypotheses, tests which of several plausible explanations for a complex event or trend stands up best against a battery of relevant information.

Third, become adept at role-playing. At times, as indicated, analysts will be well positioned to prepare a professional response to criticism by undertaking an open-minded assessment of the *policy critic's paradigm* (i.e., mental model) on a contentious issue. However colored by political considerations it may at first seem to the analysts, deconstruction will help identify the critic's assumptions, evaluation of evidence, and calculations of likelihood. Once this information is at hand, the analysts may see a path toward revision of their own assesssment that both protects objectivity and enhances utility.

Fourth, lean forward professionally with action analysis. Analysts should not hesitate to respond to criticism about unhelpful analysis by changing the question from the one they initially believed should be addressed to one policy critics call for—again a posssible path to both objectivity and utility. Often the shift, as previously indicated, is from what is the most likely interpretation of an event or relationship or the most likely future path of development, to depiction of the direct and indirect leverage the United States has to reduce dangers and seize opportunities.

In most cases, analysts can be professionally comforted by assuming savvy administration officials, despite a politically required public optimism, know their policy initiative is facing heavy obstacles, even before the CIA assessment

elaborated the point. What is now in demand are intelligence insights for doing something about the obstacles.

An analyst once tabled an assessment that placed emphasis on the general political dynamics in country *Z*, including both domestic reform tendencies promoted by the United States and a deliberate show of independence from Washington on certain international issues. The word came back that the high-level U.S. official who had asked for the assessment "wanted to leverage the president of country *Z,* not love him."[9]

Fifth, master techniques for evaluating inconclusive evidence. More deliberate analyst attention to evaluating evidence on contentious policy issues is another promising avenue for stripping tradecraft complaints from policy-maker criticism of analytic performance. Careful consideration of alternative meanings of gaps in information, especially regarding suspected programs to develop weapons of mass destruction (WMD), can help build credibility with critics.

Analysts can organize and asssess what is known and unknown to determine, for existance, whether the gaps in expected indicators more likely represent limited U.S. collection and substantial D&D, an innovative approach to WMD development, or nonexistence of a concerted development effort. The aforementioned analysis of competing hypotheses is well suited to provide an externally structured (that is, minimally subjective) competition to see which explanation is the most and least compatible with available related information.

Sixth, use estimative terminology carefully. Analysts have a professional obligation in maintaining integrity while supporting the policy-making process to avoid compounding substantive uncertainty with linguistic confusion. This is essential to managing tensions on sensitive issues. To deter both misunderstanding and manipulation of judgments, analysts should avoid vague estimative phrases such as "real possibility" and "good chance." Though not without risk of an exaggerated precision, analysts should aim to set boundaries to key judgments (e.g., "we judge the likelihood of *development Z* to be low—on the order of 10 to 20 percent"). On controversial issues analysts should also avoid nonfalsifiable judgments such as "it is possible," "suggests that," and "according to reports." They should provide instead an evaluation of the authenticity, adequacy in terms of completeness and consistency, and significance of the evidence. And when no confident judgment can be made, analysts sould say so directly.

As previously indicated, policy officials tend to stick to initiatives even against long odds. An assessment that calculates an estimated probability of a development at, say, roughly 80 percent is making transparent a roughly 1-in-5 prospect of being wrong. An assessment that develops the longshot case using plausible alternative assumptions and evaluations of the evidence, as well as the analyst's preferred 4-in-5 prospect can serve professionally to provide distinctive value added to policy-maker criticis without sacrifice of analytic integrity.

Seventh, be responsive to criticism but not at the cost of objectivity. As long as an analytic unit believes it has done its homework in evaluating evidence and in considering alternative explanations and projections, it should stand by its

estimative judgments even if policy-maker criticism persists or intensifies. But the unit should also work to ensure continued access to and credibility with critical clients by varying the focus and perceived utility of its deliverables. Analysts should consider the following "1-3-1" approach to an issue of critical policy import on which they are engaged in producing nearly daily assessments.

- Once a week, issue an assessment that features a net judgment, whether or not the one favored by policy officials. Include a credible accounting of the impact of recent developments and reports.
- Several times a week, put the net judgment approach aside and employ action analysis to address tactical dangers and policy opportunities on which direct and indirect U.S. leverage could be applied.
- Once a week, change the question via the tradecraft of alternative analysis, in order for both analysts and policy makers to examine the issue from another angle, for example: *what-if analysis* (what policy makers would see, if the likelihood of development *X* increased), *risk-benefit analysis* (the adversary's estimated calculations affecting its motivation for and ability to engage in development *X*), and *if-then analysis* (implications of the advent of a high-impact, low-probability development regarding *X*).

Finally, what of the danger that analysts' efforts to curb their own substantive and cognitive biases will generate deliverables that provide unwarranted support to the clients' biases and political agenda while weakening respect for the production unit's professional judgment?

There may be no win-win answer to the vulnerability of unintended consequences of attempts at professional accommodation of the tensions attending policy-maker criticism of analysis. Policy makers, for example, have been known to tear off the cover page (literally and figuratively) explaining the main view of the analysts and the context for presenting an alternative view—and then citing the latter as the Agency's judgment.

But avoidance of the initiatives recommended above for professional accommodation of criticism and instead countering policy-maker exaggeration of certitude with analyst exaggeration will help neither camp. As a rule, a blending of deliverables that indicates an openness toward alternative interpretations with regular affirmation of what analysts believe to be sound, if vulnerable, judgments will protect analytic professionalism, maintain credibility with and access to the policy clients, and best serve the national interest.

Analysts and production units unsure of how to proceed when confronted with policy-maker criticism with political overtones should engage the Agency's Ombudsman for Politicizaton and other detached veteran practitioners for help in identifying the best professional response. Agency training courses that include case studies on managing tensions would also help prepare analysts and managers for their initial exposure to friction with their policy-maker clients.

Largely as a result of internal as well as external reviews of flawed analytic performance regarding judgments about Iraqi WMD arsenals and programs under the Saddam Hussein regime, many recommendations for dealing with criticism of analysis by policy officials similar to those outlined above have been adopted or reinforced as tradecraft doctrine by CIA's senior leadership. As this chapter was written (March 2006) the difficult tranformation from doctrine to practice was under way.

POLICY MAKER PREROGATIVES—AND THEIR LIMITS

The preceding two sections of the chapter addressed: (1) analysts' professional prerogative to stick to their best judgment after testing it for soundness, no matter the intensity of policy-maker criticism; (2) their obligation to mitigate tensions via alternative means of support to policy clients, such as action analysis; and (3) the breach of professionalism entailed in both deliberate and unintentional politicization of analysis.

What about the rights and wrongs of the admittedly more powerful policy-making camp? The national interest is best served when the two camps work together to combine sound intelligence analysis with sound policy analysis. That said, when the two camps clash, what are the prerogatives of policy officials and what actions should be considered a breach of their professional obligations?

The questions and answers that follow are an attempt by the author, long an observer of the relationship but a member of the analytic camp, to set ground rules for policy officials that would enhance the benefits and temper the dangers of tensions in analyst–policy maker relations.

1. Are policy makers entitled professionally to reach, publicize, and act upon estimative judgments that diverge from intelligence assessments on a national security issue?

Yes. As indicated throughout this chapter, intelligence analysis, especially inherently fallible interpretative and predictive analysis, is an input to and not a substitute for policy analysis. Policy makers as analysts take account of other providers of information and judgment, and also bring their own, often considerable, experience, insights, and biases to the difficult tasks of policy formulation and implementation, for which they must take ultimate responsibility.

2. Are policy officials professionally entitled to ask intelligence analysts to take another look at their estimative judgments (e.g., to review assumptions, evidence, and argumentation)?

Yes. Policy makers are commissioned to devise, promote, and enact the president's national security agenda. They know when a policy consensus is taking shape and the time for action is approaching on issues, despite intelligence assessments that sound a caution. Yet officials, especially those with an appreciation

for the distinctive role of intelligence analysis, hesitate to ignore intelligence findings and estimative judgments that call into question the underpinnings for U.S. initiatives. One response in these circumstances is to ask analysts to go back to the drawing board. Furthermore, from the point of view of the national interest, well-articulated criticism of analysis is much preferable to inadequate guidance for the execution of intelligence deliverables and scant attention to the assessments once delivered.

3. Are policy makers professionally entitled to urge analysts to review and revise their confidence levels in analytic judgments?

Yes. For the same, usually healthy, reasons, one analyst or intelligence agency challenges another's conclusions on whether a shrouded current relationship or indeterminate future development is *nearly certain*, *probable*, or *unlikely*, policy makers may ask analysts to rethink their degree of confidence in a judgment. Once again, the answer assumes estimative judgments are inherently subject to error and that policy makers' criticism of analysis is more useful to sound performance than their ignoring of analysis. Needless to say, intelligence analysts are professionally bound to stick to judgments on probability that survive their critical review; and intelligence professionals must take care not to allow the pressure of a process of repeated requests for revision to move the bottom line further toward one supportive of policy than the analysts' tradecraft would justify.

4. Are policy makers professionally entitled to ask analysts to provide well-argued alternatives to their studied bottom-line judgments (e.g., devil's advocacy)?

Yes. Policy officials are at least as wary of the consequences of policy failure as analysts are of intelligence failure. They are professionally entitled to task analysts to use their skills and resources to present for consideration alternative or multiple views of a complex and uncertain issue. At times a call for, say, devil's advocacy may be a caution against the perils of groupthink, especially in cases in which policy makers agree with the analysts' judgments. At times the policy maker's motive will be to move Agency analysis to closer alignment with his or her own thinking. As long as rigorous analytic tradecraft norms are adhered to for whatever form of alternative analysis is solicited, and the analyst's preferred bottom-line judgment is firmly attached to the deliverable, intelligence professionals should welcome the opportunity for customized service to their policy-making counterparts.

5. Are policy makers professionally entitled to ask analysts to change the question they address (say, from whether a development is likely, to how it might occur)?

Yes. Once an administration adopts an initiative, policy makers tend to move forcefully into their action-officer mode and have limited interest in analysts' views, based on the latter's reading of the evidence, on whether the policy is likely

to succeed, much less whether the policy was wise to undertake. Policy officials have a job to do—to make the policy work. They are professionally entitled to ask intelligence analysts to provide action or implementation analysis—that is, expert assessment of opportunities for moving the policy forward and of specific dangers to be avoided, taking account of insights into the adversary's strengths, weaknesses, and "game plan."

6. *Are policy makers professionally entitled to seek analytic judgments from sources other than CIA and other U.S. professional intelligence organizations?*

Yes. No matter how strongly intelligence professionals would prefer otherwise, policy officials, in pursuit of their policy-making and political goals, have a right to rely on whatever sources of information and insight they choose, either to supplement or to substitute for the support they get from intelligence professionals. This includes use of business, academic, and other nongovernmental sources; their own staffs, whether configured as a policy-making or intelligence unit; and also, as has happened, foreign intelligence services. Policy makers, in short, are entitled to reap the benefits of as complete and varied a set of substantive inputs as they can command as they undertake the arduous task of managing an uncertain and often perilous national security issue. If policy makers use different sources of analytic support simply because they want more cordial answers than those provided by intelligence professionals, then the policy officials must bear the burdens of self-deception, policy failure, and political censure when such outcomes prove to be the case.

7. *Are policy makers professionally entitled to attribute to intelligence analysts judgments that overstate or understate analysts' confidence levels?*

No. Once a studied, clear, and (if challenged) revisited statement of likelihood regarding a development, relationship, threat, or opportunity is established by Agency analysts, policy officials can attribute it to intelligence in order to buttress their own views, or reject it in favor of their own alternative statement of likelihood. But they do not have the authority to attribute to intelligence professionals an estimative judgment the latter do not hold.

8. *Are policy makers professionally entitled to force analysts to alter their best estimative judgments?*

No. As already acknowledged, policy officials are entitled professionally to reject intelligence assessments and reach and promote their own estimative judgments (Question 1, above), and are also entitled to urge analysts to rethink and recast Agency intelligence judgments (Question 3, above). That clarified, under no circumstances are policy officials professionally entitled to force intelligence analysts to change estimative judgments. Obviously, there are risks to treating as inviolate intelligence judgments that are contrary to policy preferences. Events may prove the analysts to be wrong. Congressmen may complicate the funding and execution of an administration's strategy and tactics by

using intelligence findings and estimative judgments to block or modify policy initiatives. Unauthorized leaks to the media of intelligence positions may create an untimely public debate over policy. These circumstances can cause a run-up in immediate costs ranging from embarrassment of the administration to the thwarting of what history may judge to have been a sound policy initiative. But the long-term costs to the integrity and morale of intelligence professionals of forcing them to change their judgments will likely cause much greater harm to the national interest by weakening a vital arm of the national security establishment.

9. *Are policy officials professionally entitled to use the media to criticize intelligence analysts' competence, in an effort to protect an administration from congressional and public criticism of a policy initiative?*

No. As argued in this chapter, policy officials are entitled, indeed encouraged, to criticize through government channels either a specific body of analysis or intelligence tradecraft generally. Furthermore, as policy professionals, they are entitled to raise publicly their criticism of analysis as long as it is couched in analytic terms and is not, in effect, a politically motivated *ad hominem* attack. That is, as policy professionals, they are not entitled to criticize publicly a careful body of intelligence work and the credentials of the analysts who produced it merely to relieve themselves of the burden of credible defense of their own contrary judgments. In principle, nearly all parties to the uniquely American system for making national security policy proclaim the value of maintaining the integrity of intelligence analysis. A practice of trying to leverage a congressional vote or public debate on a policy initiative by criticizing the credentials of analysts who produce uncongenial analysis undermines the principle.

10. *Are policy officials professionally entitled to apply pressure on Agency leaders to remove from a production unit a manager or analyst responsible for assessments with judgments policy makers see as biased, wrong, or otherwise unhelpful?*

No. Analysts and their managers should be judged by Agency leaders solely in terms of professional credentials and adherence to analytic tradecraft norms, including good-faith efforts to respond to tradecraft criticisms by policy officials through the various means outlined earlier in this chapter (e.g., key assumptions check, devil's advocacy). The challenge of reaching sound analytic judgments amidst the perils generated by substantive complexity and uncertainty should not be compounded by a requirement for "political correctness" or fears about job security.

11. *Are policy officials professionally entitled to request Agency analysts to engage in policy advocacy, for example, to produce a "white paper" that is released as an intelligence product?*

No. Agency analysts may assist by providing information for the production of a white paper, but this and other formats of policy advocacy must be issued

under the seal of a policy-making department or staff. The role of Agency analysts is to provide analytic support to policy planning and implementation by administration officials—and not to make, advocate, or criticize policy. Again, the long-term importance to the national interest for Agency analysis to be and be seen as a source of substantive objectivity as well as policy utility far outweighs any short-term political advantage gained from using an adulterated form of intelligence analysis to gain public or congressional support for a policy initiative.

CONCLUDING THOUGHTS

What about enforcement of these or any other set of ground rules aimed at moderating tensions in analyst–policy maker relations? U.S. experience has shown that presidents and their inner circles from time to time will play by their own rules. Agreed prerogatives and constraints and authoritative calls of "foul" might nonetheless serve well over the long haul, if only to evoke second thoughts about ignoring a transparent set of rules for improving both intelligence analysis and national security policy making.

Presidential administrations already have an instrument in place for monitoring the adequacy and quality of intelligence analysis, along with all other intelligence functions. The President's Foreign Intelligence Advisory Board (PFIAB) is well situated, both to help shape the ground rules and to monitor for analyst compliance. Over the decades, PFIAB members—former administration officials, members of Congress, and military and business leaders—collectively have commanded formidable knowledge about analysts and policy makers. And as a rule, PFIAB staff reports on analytic performance have been noted for both independence and insight.

For the Agency, the Ombudsman for Politicization has served since the early 1990s to educate new analysts about professional standards, to monitor for politicization, and to counsel analysts about the concerns they raise on the issue. Over the years, the Ombudsman, selected by and serving at the pleasure of the Director for Intelligence, has been a highly qualified former intelligence manager serving part-time as an independent contractor.

The following recommended changes relating to the Ombudsman are intended to strengthen both the educational and protection functions, including by participation in shaping ground rules and more active monitoring for compliance on the part of policy officials as well as intelligence professionals.

- Change the position name to Ombudsman for Analytic Professionalism (OAP*)*. The professional obligations for analysts in the management of tensions involve more than the avoidance of policy or political bias.
- Provide the OAP with a small staff. The rise in importance to U.S. national security of countering weapons proliferation and terrorism—issues on

which conclusive evidence will be a rarity—is likely to increase tensions over the meaning of available information and thus the demands on the OAP.
- To ensure the independence of and enhance analyst confidence in the OAP, have the newly instituted Director of National Intelligence nominate and Congress confirm the title holder to serve a fixed term of five years.
- To help hold policy makers as well as analysts accountable in their management of tensions, require the OAP to provide the intelligence oversight committees of Congress with periodic reports on the compliance of both camps with agreed ground rules.

This chapter, by design, has mentioned Congress only briefly, although it is the third side of the triangle that constitutes the U.S. system for making and implementing national security policy. Yet for any set of ground rules for governing analyst–policy maker relations to have a lasting impact, Congress, on its own or in response to public demand, must take action to promote and monitor such an initiative. The goal, one last time, would be to ensure that the inevitable tensions between Agency analysts and administration officials are managed to the benefit of the national interest.

NOTES

All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the CIA or any other U.S. government agency. Nothing in the contents should be construed as asserting or implying U.S. government authentication of information or Agency endorsement of the author's views. The material has been reviewed by the CIA to prevent the disclosure of classified information.

1. Quoted in "Rumsfeld on New DoD Intelligence Team," *Early Bird* (newsletter), Department of Defense (October 25, 2002), available at http://www.defenselink.mil/news/Oct2002/t10242002_t1024sd.htm

2. Author's interview with Paul Wolfowitz, "Paul Wolfowitz on Intelligence-Policy Relations," *Studies in Intelligence* 39 (Langley, VA: Central Intelligence Agency, 1996).

3. Author's interview with CIA analysts present when the remark was made at CIA Headquarters, Langley, VA, in 1982, cited in Jack Davis, *Tensions in Analyst-Policymaker Relations: Opinions, Facts, and Evidence,* Occasional Papers, CIA, Kent Center 2 (2003), p. 3.

4. Comment made to the author in April 1980, CIA Headquarters, Langley, VA, cited in Davis, "Tensions," p. 3.

5. Author's interview with Paul Wolfowitz, "Paul Wolfowitz."

6. Intelligence Side Letter [to Congress and the Director of Central Intelligence], Report of the Commission to Assess the Ballistic Missile Threat to the United States (March 18, 1999).

7. Quoted in "Rumsfeld on New DoD Intelligence Team," *Early Bird.*

8. *Editor's note:* After the Bay of Pigs failure in 1961, President Kennedy observed, "There is an old saying that victory has a hundred fathers and defeat is an orphan," cited in Arthur M. Schlesinger, Jr., *A Thousand Days: John F. Kennedy in the White House* (Boston: Houghton Mifflin, 1965), p. 289.

9. Author's recollection of a 1973 incident, cited in Davis, "Tensions," p. 6.

NOTE ON SOURCES

The views on and of policy officials are based on remarks made at press conferences and in unclassified statements in reports by governmental commissions, media interviews, and discussion forums. Note, for example, the following publications that are available on the CIA website (http://www.cia.gov). Note also, the unclassified source cited for the evaluation of and recommendations for analysts by the Missile Commission, chaired by Donald Rumsfeld.

BIBLIOGRAPHY

Armstrong, Fulton T. "Ways to Make Analysis Relevant But Not Prescriptive," *Studies in Intelligence* 46 (2002).

Davis, Jack. "[Ambassador Robert Blackwill] A Policymaker's Perspective on Intelligence Analysis," *Studies in Intelligence* 38 (1995).

———. "Paul Wolfowitz on Intelligence-Policy Relations," *Studies in Intelligence* 39 (1996).

Report of the Commission to Assess the Ballistic Missile Threat to the United States: Intelligence Side Letter [to Congress and the DCI], March 18, 1999.

The views on and of intelligence analysts and on the analyst–policy maker relationship generally are based on the following unclassified publications that, unless otherwise indicated, are available on the CIA website (http://www.cia.gov).

BIBLIOGRAPHY

Davis, Jack. *Analytic Professionalism and the Policymaking Process: Q&A on a Challenging Relationship*, Occasional Papers, CIA, Kent Center, Volume 2, No. 4 (2003).

———. "Combating Mindset," *Studies in Intelligence* 36 (1992).

———. *Improving CIA Analytic Performance: Analysts and the Policymaking Process*, Occasional Papers, CIA, Kent Center, Volume 1, No. 2 (2002).

———. *Improving CIA Analytic Performance: DI Analytic Priorities*, Occasional Papers, CIA, Kent Center, Volume 1, No. 3 (2002).

———. *Sherman Kent's Final Thoughts on Analyst–Policymaker Relations*, Occasional Papers, CIA, Kent Center, Volume 2, No. 3 (2003).

———. *Tensions in Analyst-Policymaker Relations: Opinions, Facts, and Evidence*, Occasional Papers, CIA, Kent Center, Volume 2, No. 2 (2003).

———. "Facts, Findings, Forecasts, and Fortune-telling." In *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, ed. Roger Z. George and Robert D. Kline (Washington, DC: CIA, 2004).

Heuer, Richards J., *Psychology of Intelligence Analysis.* (Washington, DC: CIA, 1999).

9

"THE CUSTOMER IS KING"

Intelligence Requirements in Britain

MICHAEL HERMAN

INTELLIGENCE HAS TO DO FOUR THINGS TO be useful. It has to provide governments with information, assessments, and forecasts on the right subjects. It has to deliver them at the right times and in the right ways. It needs to be close to government, with a credibility that means that what it says is taken seriously. Most important, what it provides should be correct or, at the very least, better than the information and conclusions government's decision takers could muster without it. The four are interrelated, but this chapter concentrates on the first: covering the right subjects.

The need to do this applies to any of government's information systems. Intelligence is just one of them, along with diplomatic reporting, statistics, and the other official sources that add to what is publicly available. It has its comparative advantages over the others on matters of secrecy and national security, yet compared with them it is secretive, expensive, more politically embarrassing, and difficult to monitor and control. Democratic governments must be satisfied that it is properly directed, not the rogue elephant that the CIA was memorably—and unfairly—said to be in the congressional inquiries of the 1970s. It should provide what government asks for. But how can this be assured?

This is a modern problem. In the centuries before government became specialized and institutionalized there were no intelligence agencies. Spies got their directions from the ministers or commanders they served, and they were paid by results. There was a similar clarity within government service; the British consuls in foreign ports who observed local naval preparations in the late 17th and 18th centuries reported directly to the Admiralty Secretaries who told them what they wanted. The small European "Black Chambers" that intercepted and deciphered foreign dispatches reported directly to their monarchs and chief

ministers. Permanent military and naval intelligence staffs were created in the following century, but they still served their own departments or commanders. Intelligence had not begun to serve multiple parts of government, and the problems of directing it had not appeared.

But by the early 20th century its covert collection was becoming a matter for specialist agencies, not subordinate to any single part of government. Around the mid-century these became further recognized in the anglophone countries as a collective entity—an "intelligence community," with its own identity and structure. Intelligence at both levels was apparently freestanding, distinct from mainstream government, and opaque within its ring of secrecy. It existed to meet the needs of multiple government departments, but its relationship with them had become one of equals, instead of a subordinate "service" to a particular boss. The relationship became described in private-enterprise terms, as one between "producers" and "customers." ("Customers" might now be described as "stakeholders," a term of political discourse introduced under the present British government, but the producer-customer analogy is well entrenched and is used here.) Customers no longer ran their own intelligence, so what was going to ensure that under its new management it did what they wanted?

In Britain the question first arose in 1909 when the Secret Service Bureau was created to develop agent-running on behalf of the Admiralty, War Office and Foreign Office. It was then posed for intelligence as a whole when the wartime Joint Intelligence Committee (JIC) became part of the peacetime machinery in 1945. The British response at both levels was the concept of government's "requirements," originally on a small scale to secure the interests of particular customers, but subsequently as a comprehensive intelligence discipline. Requirements became accepted as intelligence's driving force, and a system for managing it.

This still applies today in the United Kingdom, perhaps to some extent in the United States. Requirements as a system presents customers' needs, but they are needs adapted to some formality. They are not just shopping lists of requests or "blue-sky" hopes, but are needs tailored to what intelligence can provide or may be capable of providing. They resemble the "operational requirements" that drive military weapons procurement, with their connotations of "demand by authority,"[1] practicability, and conformity for those on whom they are laid. For intelligence they are to a degree a directive mechanism, and in recent years they have also become a touchstone of legitimacy. No respectable intelligence agency or community is now complete without them.

What follows here outlines how this idea of requirements evolved in Britain in the period up to the end of the Cold War, plus some comments on American practice, and references to what is known of recent British developments. It is based on a mixture of the author's recollections and such published evidence as is available.

PRODUCERS, PRODUCT, AND CUSTOMERS

British intelligence producers were then (as now) of two general kinds, and produced two kinds of product. Some were specialist information collectors, each expert in its own particular *techniques* and a producer of "single-source" output based on its own material. The main agencies were Government Communications Headquarters or GCHQ for signals intelligence (SIGINT), the Secret Intelligence Service (SIS or MI6) for human intelligence (HUMINT), and the Joint Air Reconnaissance Intelligence Centre (JARIC) for imagery intelligence (IMINT).

Others were government's experts on their designated *subjects*, and their output on them was "all-source" analysis of all relevant information. The largest all-source producer was the Defence Intelligence Staff (DIS), and all-source assessments for top government were provided by the JIC and its Assessments Staff in the Cabinet Office.

There were also those that were both collectors and all-source specialists. The Security Service (MI5) was both a collector and all-source assessor on espionage, terrorism, and similar threats, and the DIS also ran some collection and controlled JARIC. This mixture of collection and analysis organizations, and some doing both, was also found in the much larger American community of the time. It still is.

All were producers, but their single-source and all-source product differed in kind. It is tempting to say that the collectors produced "facts" and the all-source organizations produced analysis and judgment: that the collectors collected foreign secrets and the analysts studied them. But this is an oversimplification: analysis ran through the whole intelligence process. Nevertheless, the differing single-source and all-source *responsibilities* were reflected in the two kinds of product. Collectors produced "good facts," as meaningful as they could make them from their own material; the others produced authoritative judgments and "big pictures."

Both kinds of product went to customers, as shown in the diagram of the intelligence process shown in Figure 9-1. Customers outside intelligence—those on the right-hand side of the diagram—received both single-source and all-source product. The proportions of the two varied between different customers and their different situations. On the one hand, military commanders had intelligence staffs who briefed them on an all-source basis, so they had little reason to read single-source material themselves; the same may now be true of those taking operational decisions on counterterrorism. On the other hand, diplomats were usually their own intelligence analysts and needed single-source intelligence to add to the other information they had. The same applied to other civil departments. JIC reports were limited to subjects of importance for top government, usually those of interdepartmental concern. In sheer quantity most of the intelligence reaching customers was single-source material reported in detail; only certain subjects got the more consolidated all-source treatment.

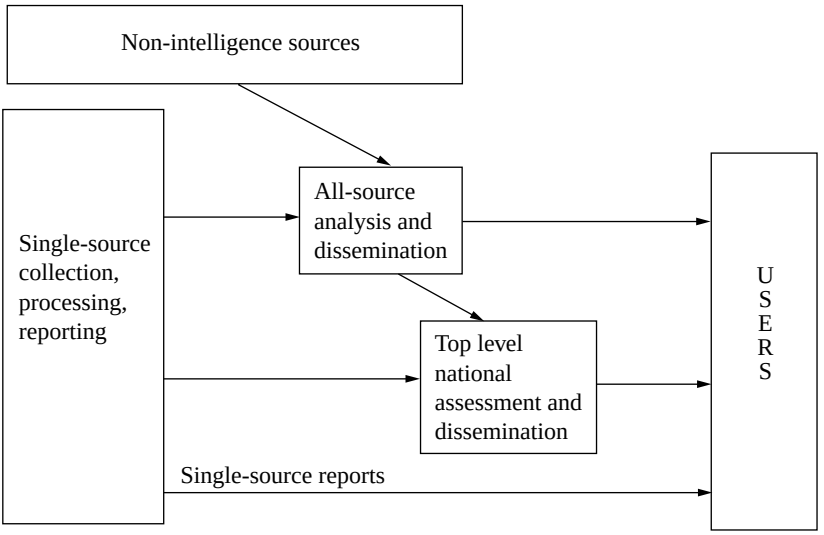


Figure 9-1. Complete Intelligence Process

Source: From Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996), p. 103.

That was the pattern of production for which the idea of requirements developed. As the diagram shows, production was geared to three different producer-customer relationships:

- All-source producers and nonintelligence customers
- Single-source producers and nonintelligence customers
- Single-source producers and all-source intelligence customers

Requirements in the third category could have been treated separately as a matter of intraintelligence management, but in practice they were rarely separated from the first two, those of intelligence and the "real" (nonintelligence) customers. A result was that little distinction was often made between the rather different needs of all-source analysts and those who used intelligence for policy or action.

Thus, by the second half of the 20th century intelligence was already a large-scale information system, responding in varied ways to the needs of many different customers and becoming more elaborate. Requirements developed as what seemed a necessary mechanism for coping with the scale and complexity as they increased. How they evolved, and with what effect, can now be considered.

DEPARTMENTAL REQUIREMENTS

Scale and complexity were not the issue when the Secret Service Bureau was created to provide HUMINT for the Foreign Office and Service Ministries. The

concern of these departments was to ensure that their individual interests would be met by the new organization. As put by Philip Davies in his work on what later became the SIS, they "were almost exactly as unwilling to delegate responsibility for spying to a separate agency as they were unwilling to go about doing it themselves and risk getting caught." They regarded the Bureau's independence as a matter of cover and convenience, to satisfy the proprieties of the time that respectable departments of state should not engage in spying. The Bureau was a "screen, armature or servant,"[2] unsatisfactory without some way of nailing it down to meeting their individual needs. Hence it was designed so that, while part of it ran agents, the other part had representatives of the Admiralty and War Office intelligence departments (though not the Foreign Office) to direct its targeting and exploit the results. To an undefined extent it was designed to be partly run by its customers. In bits of modern jargon it might be called a matrix organization, operating by customers' "pull" rather than producers' "push," with "embedded" representatives of the "stakeholders" to secure their interests. Requirements from the outset had these suggestions of authority.

British agent-running greatly increased during World War I and was conducted by multiple agencies. Nevertheless, the device of customer representation was preserved when the foreign intelligence part of the 1909 organization was put on a postwar basis in 1919 as the SIS. A separate "Requirements and Circulating" section was established as part of its basic organization. To quote Davies again: "The Requirements side began life as a cluster of consumer-liaison sections. . . . SIS's largest and most powerful consumers—the War Office, Admiralty, Foreign Office and, later, Royal Air Force—seconded sections of their own intelligence branches to SIS to lobby for their partisan interests."[3] This was modified as time went on, notably by filling more of these posts by SIS's own staff. But the doctrine remained that the SIS's production side "mounts operations in response to specific demands laid on it by a tasking, validation and dissemination apparatus referred to as its 'Requirements' side."[4] Whitehall's faith in this idea of customer involvement was illustrated in 1942 when the answer to the armed services' dissatisfaction with SIS's product was for them to appoint more senior representatives as deputy directors, known by their hosts as the "service commissars."[5]

These senior appointments did not continue for long, but the Requirements organization remained important in SIS's postwar structure and retained equal status with Production. Formal, articulated customer requirements became a major part of the service's modus operandi. But as the Cold War developed, with its secrecy, deception, and double-agents, the original Requirements role of reviewing draft reports against customers' needs was extended to validating their quality and reliability by bringing its second opinion to bear on Production's view of its sources. Late in the Cold War this started to change for reasons of economy and efficiency, and in the course of the 1990s Production took over the whole process. The Butler Committee of 2004 that investigated British performance over Iraqi weaponry was advised that this demise of Requirements' validation was

responsible for the misleading SIS reports that contributed to the JIC's errors, and it was assured that the earlier arrangements were being restored: a return to the old principle of Production-Requirements duality, though not for the original reason. It is of interest that the CIA's Directorate of Operations has never adopted this British-style duality for managing its HUMINT.

British SIGINT evolved differently. It hardly existed in 1909 and was no part of the Secret Service arrangements of that year. It developed on an extensive scale in World War I as separate efforts under the War Office and Admiralty to meet single-service needs, and the Admiralty also produced diplomatic decrypts for the Foreign Office and joined with the War Trade Department in exploiting cable traffic for continental blockade. In 1919 a national SIGINT organization was created as the Government Code and Cypher School (GC and CS), and two years later was placed under the head of SIS's authority, though with much practical autonomy. On the HUMINT pattern, parties of the three armed forces were included in its organization. The armed forces maintained their own interception efforts, and at least in the 1920s it was expected that much of GC and CS's effort would revert to the individual services in war.

Little has been written about its interwar machinery for handling customers' needs, though it does seem that GC and CS received SIS's customer requirements. As little foreign military traffic was intercepted, military requirements were not a live issue. The main output was decoded diplomatic messages, on which there was productive contact with the Foreign Office, illustrated in a protest from Lord Curzon, the Foreign Secretary, about a plan to move the code-breakers from premises close to Whitehall to a building two miles away. He argued that frequent visits to Foreign Office desks were essential; the code-breakers often needed to draw on Foreign Office information, and the value of their decodes could be time-sensitive: "In many cases the same official visits the F.O. every day, not infrequently several times a day. In cases of difficulty the same official has been known to pass from the School to the F.O. and back 5–6 times a day."[6] This has all the marks of special pleading, but it shows close contact; and it was the producers who visited the customers, not the other way round.

In World War II the situation changed radically. SIGINT became the most important source of intelligence, meeting customer demands throughout the armed forces and government departments. It became a worldwide effort orchestrated by GC and CS at Bletchley Park. Yet it was still complicated by single-service "ownership" of significant parts of the effort, and there was a constant tug between the technical arguments for centralization and the individual armed forces' wishes to exploit "their" SIGINT under their own control.

Wartime Bletchley was indeed a mixed service and civilian organization, and to its service customers there seemed clear analogues with HUMINT. Just as they saw SIS as the expert at running human sources but controlled the results, they conceded GC and CS's expertise in code-breaking but argued that the military parties who were exploiting the decrypts at Bletchley should be under their command. SIGINT could well have developed in that way, but in the course of

1942 it was accepted that the service parties should be controlled by Bletchley. From this the principle was gradually accepted of a single national SIGINT agency with responsibility for the complete SIGINT process: a principle that became a foundation for postwar British SIGINT, and for the American National Security Agency when it was created as its analogue in 1952.

Thus SIGINT requirements never acquired the same salience as for HUMINT. Bletchley's wartime organization evolved around targets and subjects rather than the dyarchy of Production and Requirements. Yet conflicts between competing customer priorities had to be resolved somehow. Bletchley was supervised by a senior interservice Board that might have done this, but in practice it came to be accepted that GC and CS "should carry out without reference to the Board the day-to-day work of reconciling the interests of the services, supervising the programme of the British Sigint centres throughout the world and settling the issues which arose from the ever-expanding collaboration between the British and American Sigint authorities."[7]

How did this come about? It happened from the middle of the war onward, a period of increasing success, when SIGINT abundance had replaced scarcity. Customers had few incentives to rock the boat. Perhaps the young men who juggled daily with Bletchley's resources to break the many German keys had the priestly aura of miracle workers. Perhaps their sports jackets and flannels proclaimed a civilian insulation from parochial single-service interests. It now seems remarkable that Bletchley's authority was accepted with so little controversy, but it happened. "In Whitehall recognition of its [Bletchley's] resourcefulness dissolved the barriers of jealousy and incomprehension which had initially kept the civilians at arm's length and separated the producers of Sigint from those responsible for making the best use of it."[8]

That was the wartime situation. After 1945 GCHQ, the successor of GC and CS, initially adopted a functional organization that included a powerful requirements, reporting, and customer liaison division that may well have been modelled on SIS's "Requirements." Perhaps it seemed that after Bletchley's wartime improvisation the new agency should have a "proper" peacetime structure of that kind. But this reverted after a few years to more target-based arrangements. Customer requirements figured in the professional in-house jargon of the rest of the century, but their most concrete application was in a useful directory: if material on a particular subject became available, which customers should receive it?

There was indeed some peacetime representation of military customers on the 1909 model, but this was at a relatively low level. The armed forces became more pressed for manpower, and more was left to the civilians. Higher level representation made a limited appearance much later, after the end of the Cold War; the first Gulf War and military deployments in the former Yugoslavia had pointed to relearning wartime lessons about support for military operations, and a senior army post was allocated to liaise for this purpose. But this did not lead to wider embedding. Indeed, the trend became to export more SIGINT liaison officers to customers, not the reverse.

For other intelligence producers the problem of choosing between particular customer interests hardly arose. The Security Service succeeded the defensive, domestic part of the original Secret Service Bureau in 1921 with responsibilities that eventually covered counterespionage, countersubversion, and counterterrorism; but it always saw itself as a security service, not an intelligence producer. It often claimed that it was "self-tasking." As for JARIC, it was not regarded as a national agency serving all national customers on the pattern of its American counterpart but was handled as a military institution that did as it was told by the DIS. The DIS itself was equally defense-oriented, and the formal requirements laid on it were in the name of the Chiefs of Staff. The JIC as the top-level producer was regarded as *sui generis*, not covered by the requirements procedure it established for others, to be described shortly.

Thus, securing individual customers' requirements was an issue when British secret intelligence was first institutionalized, but its significance diminished except to some extent for SIS. Coping with competing bids came to be handled on the whole as part of normal day-to-day business. But as requirements settled down at this level, they became important at the new, post-1945 "national" level of the JIC and intelligence as a whole. Intelligence could now be considered as a community. The question became: what was required of it from customers collectively?

THE SHIFT TO COLLECTIVE REQUIREMENTS

Thinking of requirements in this way may have had its origin in the British planning for postwar intelligence that began in 1943. A study of government's future needs was drawn up at that time and may have been the prototype of the subsequent JIC reviews of requirements that were produced after 1945. The titles were varied: At one time they were "intelligence targets," but they were later standardized as "requirements and priorities." They were originally issued at irregular intervals, but in time they came to be produced by the JIC as an annual routine, and subsequently presented for approval by the (official) Permanent Secretaries' Committee on the Intelligence Services (PSIS) that considered intelligence budgets. Subsequently a further layer of approval was added with the creation of a ministerial committee that at least nominally approved requirements along with budgets. Requirements authorized in this way became the main prescription of what the British agencies should do, and by implication not do. They have retained this role: the JIC's latest published responsibilities include the obligation "to submit, at agreed intervals, for approval by Ministers, statements of the requirements and priorities for intelligence gathering and other tasks to be conducted by the intelligence Agencies."[9]

This was a logical complement of a national intelligence community and could be justified on various grounds. Intelligence as a national resource should be orchestrated to meet national needs. Those approving budgets should know what targeting they were endorsing. On major threats there should be an intelligence

strategy, as suggested in the memorable British recommendation of 1947 that the intelligence attack on the Soviet target should be mounted as a "campaign."[10] In reality it is doubtful whether any of these justifications was put forward. The long-standing significance of requirements for the SIS probably paved the way for producing them through the JIC, and this probably seemed such a commonsense use of the committee that no particular rationale was needed.

Later, however, the idea of community requirements acquired sharper teeth, as a managerial tool. Establishing intelligence's subjects might provide the framework for better evaluation of its yields, costs and cost-benefits, and more rational management. There were hopes of constructing a logical requirements hierarchy in which national requirements cascaded down to those at departmental and other levels. There were perceptions of a grand intelligence plan in which everything was costed, prioritized, and allocated somewhere to avoid duplication. The community might not be a rogue elephant, but it was a slippery octopus, and attention to requirements seemed one way of getting hold of it. None of this was explicitly articulated, but at the Whitehall center it seemed the way of the future. The intelligence producers for their part supported anything that endorsed their activities and welcomed, at least presentationally, anything that helped them to decide between competing customer requests—though they took every opportunity to ensure that these would not limit their operational flexibility.

It may be that this emphasis on the customer and what he wanted had some subliminal support from the military doctrine that developed in the same period of the "intelligence cycle": the process whereby the customer states his requirement; intelligence responds by collecting, analyzing, and producing; the customer amends his requirement in the light of what he receives; and the iteration continues. The cycle was put forward in many versions, but it tended to be centered on the customer (the military commander): he requested, and intelligence responded.

By the second half of the Cold War this cycle had become the basis of British and American (and North Atlantic Treaty Organization [NATO]) military doctrine for using the increasingly complex collection systems becoming available for the battlefield. It may have made little direct contribution at that time to British thinking about the JIC's requirements; it was then a military concept and the civilians' acquaintance with it was patchy. But it probably had some background influence. It probably also had rather wider currency in the more military-oriented American intelligence community: For many years it featured in the CIA's public factbook, and indeed it still does. The Cold War saw some convergence that, one way or another, intelligence was a requirements-driven process, or should be; and the cycle helped then, and has helped since, to make it the conventional wisdom.

Another prop for requirements' standing came rather later, in the final years of the Cold War and afterwards, when intelligence in Britain moved to a more public and less secretive status. The agencies' roles became defined by legislation, and requirements then fitted as a logical link between them and their translation into practice. They also came to figure in the procedure for ministerial

authorization of interception and other sensitive operations, because relevance to JIC priorities demonstrated that operations or proposals were kosher. They also became relevant to the new Intelligence and Security Committee of Parliamentarians and its remit to review the expenditure, administration, and policy of the secret agencies. With these developments it was sensible for requirements' existence and procedure to be described when official accounts of the intelligence community were made public from the mid-1990s onwards. They became part of the British edifice of intelligence legitimacy—a place that they occupy today. The foreigner has the impression that, though they are much used within the American intelligence world, they have perhaps played a rather smaller public part in the U.S. system of democratic oversight than with the British.

So requirements came to stay. But there was no single, perfect scheme for them, and they had a variable record in realizing the hopes vested in them. A complete account is not available, but some recollections can be recorded of the British experience of their development and application.

COLLECTIVE REQUIREMENTS IN PRACTICE

Questions that arose in developing requirements into a system included the following:

- As already explained, the customers for single-source reports were both inside intelligence and outside it: the all-source analysts, on the one hand, and mainstream government, on the other. Should single-source requirements cover the potentially different needs of the two?
- Linked with the first question, were requirements to be set out for both single-source and all-source intelligence, or one or the other? If so, which? Or should there be two sets of requirements and not one?
- Should the same requirements and priorities apply to all collectors, or should each of them be allocated those subjects on which it was best able to contribute?
- What allowance should be made for the availability of extensive American product? Could requirements be met by supplying foreign product, or did they call for a specifically British effort? Conversely, should the American interest in special British contributions (for example, from Hong Kong's special "window" onto China) count as requirements, and with what priority?
- Irrespective of their precise scope, what directive force should requirements and priorities actually have?

For about fifteen years after the end of the Cold War such worries could be kept on a back burner. (A draft JIC report on "Sigint Requirements—1948" issued in May 1948[11] did indeed deal with one source, but as far as can be

recalled this was not repeated.) In the author's recollection the norm up to the 1960s was to produce fairly broad lists applying to intelligence as a whole, with relatively simple prioritization. These probably sufficed for airing the pressing question of the 1950s: what priority should be attached to the detailed intelligence on the Soviet armed forces needed for conventional warfare, at a time when thinking was moving toward the impact of missiles and nuclear weapons? As one side of the argument was put by GCHQ's Director in 1955, the time had come for "more intelligence that would help us in the 'cold' war, rather than the 'hot' war."[12] In the event the requirements and priorities reports of the time reflected the compromise that all aspects of the Soviet threat were important, but with some priority for strategic nuclear aspects and intelligence's role of warning.

In fact this debate continued in subdued form through much of the Cold War. Civilians regularly criticized military intelligence for unnecessary "bean counting" of Soviet military *minutiae*, while the military pointed out that it was silly for the United Kingdom to keep large conventional forces to deter the Russians if it then denied them the intelligence that might give them a chance if they actually had to fight them. How was the priority of the big effort on Soviet military targets to be compared with the smaller packets of effort on non-Soviet targets that helped Britain to "punch above its weight" politically in its decades of national economic weakness? Or with the actual conflict with Irish terrorism? The JIC's answers were compromises, as was perhaps inevitable. But its system of requirements and priorities provided some safeguards for military interests and kept everyone reasonably happy. As demanded in 1947, intelligence did wage a coordinated Cold War "campaign," even though not a dramatic one, and the JIC's requirements and priorities played their part in it.

In the 1960s, however, there were hopes of giving them additional teeth. It was a period of British intelligence reform: The three service intelligence directorates and the Joint Intelligence Bureau were combined in 1964 into the new DIS, and successive moves to improve the effectiveness of the JIC's central machinery culminated in its reorganization in 1968. Internationally the Cold War settled into a mood of détente after the Cuban crisis of 1962, and the Soviet threat seemed less pressing. It was also a period of Britain's economic decline, and its withdrawal from its imperial positions in Africa and "east of Suez." The accent everywhere was on financial retrenchment: Reduced commitments should mean intelligence economies. The conviction grew in Whitehall—related to the perception of military bean counting—that customers were getting intelligence they did not really need, or could get from nonintelligence sources. A proper scrutiny of requirements could save money.

These threads came together in serious attempt in the mid-1960s at a comprehensive JIC audit: what parts of government needed "intelligence" as distinct from other information, on what subjects, and for what purposes? Who needed what, from whom? What would emerge as rational priorities? Considerable interdepartmental effort under Cabinet Office chairmanship was devoted to a series of careful area-by-area studies, but the objective of a complete survey leading to

evidence-supported, interdepartmentally agreed conclusions remained elusive. Trying to examine everything from A to Z in a committee of differing interests was no way to reach actionable conclusions. Eventually a clever diplomat cut though the complexity to produce a commonsense report that suggested some obvious shifts of emphasis, and everyone was satisfied. This was not quite the last attempt at a review of this kind, because it was followed at the end of the decade by an attempt to audit all the overseas economic information needed by government departments and the consequential requirements for "economic intelligence." But that, too, was not a success.

Nevertheless, the interest in requirements remained, and responsibility for reviewing them was identified as belonging to the new senior post of Intelligence Coordinator, established in the Cabinet Office in 1968. Perhaps to avoid repeating the attempted JIC audit, the Coordinator was initially given some freedom to set out national priorities off his own bat, and for a period in the first half of the 1970s the JIC's annual lists of requirements were discontinued. A short-lived Cabinet Office "Central Monitoring Point" was established to consider requirements again, but it lapsed. After these experiments the system then gradually reverted to the earlier pattern of annual JIC statements. The permanent innovation was that the Coordinator remained the prime mover in the intelligence-customer consultation these entailed.

So there were no more grand investigations, but there were consistent attempts to make requirements more precise and useful. In the last decade of the Cold War, and indeed the 1990s, "value for money" was a catch phrase for governments of both parties, and seeking "better requirements" seemed an appropriate intelligence response. Those seeking value for money in Whitehall inherited the conviction that probes from the center would reveal pots of gold hidden somewhere. It may have been right, but it never found them.

One result was that what in earlier years was guidance for the whole community was focused exclusively on the main collection agencies, SIS and GCHQ, on which most of the money was spent. National requirements for the rest of the community were left in limbo. One consequence was that the requirements presented to the single-source agencies more obviously included those of the all-source analysts; the DIS was involved as a *demandeur* rather than a producer.

A second result was to be more positive about what priorities meant. A distinction was drawn between those subjects that should be targets, and those that should not be targeted but on which material should be reported if it was available as a by-product of other coverage, or from foreign liaisons. The system acquired teeth: the approval of the center was necessary before targeted collection could be initiated against the by-product category. In the last years of the Cold War the idea developed of introducing the discipline of a pseudomarket, whereby customers would bid to "pay" notionally for intelligence to meet their requirements, and intelligence budgets would depend on the bids or results; but it did not get very far.

In these ways JIC requirements remained an accepted part of the scene, as they continue to be. "Better requirements" became a mantra with those outside intelligence who had an interest in it. Considerable effort was put into improving the system. But what difference did it all make?

EFFECTS AND LESSONS

British intelligence had to have a directive of some kind about the subjects it was required to tackle and, by implication, not do so, and about priorities for tackling them. Government had to know what was authorized and demanded in its name, for democratic oversight as well as other reasons. Intelligence had to understand its remit and have community understandings about policy and strategy. The JIC was well suited to formulating requirements and priorities for these purposes, because its membership included the Foreign Office and other principal customer departments along with the intelligence community proper. It was a weakness that when the system was made more sharply focused the DIS ceased to be formally bound by it; and it was a British eccentricity that while JIC requirements applied elsewhere in the community the Committee did not apply them to itself in its role as Britain's top intelligence producer. But these oddities were more apparent than real. The JIC was good at being collegial, and its members were agreed on what they should be doing: not a negligible achievement for a committee of secret organizations.

Yet it is difficult to recall that the requirements procedure ever affected what intelligence actually did. The annual routine was taken seriously, especially after Coordinators came to give their attention to it, but there was an element of ritual about it. Lists of requirements and priorities were drawn up by intelligence and submitted to customers for collective review—the reverse of what strict logic might have suggested. What emerged reflected what intelligence was producing and customers were receiving, subject to some minor annual tweaking. It should be repeated that the JIC dispensed with the whole thing for some time in the 1970s and no one noticed the difference.

Intelligence producers' attitude to the process was mixed. It was valued if it opened new doors for discussion with customers. It might provide excuses for kicking unreasonable customer demands into touch. On the other hand producers regarded good relations with their individual customers as emphatically their own business. Any difficulties with them should be handled one-to-one; nothing good would come of letting the center get into the act. Insofar as the JIC procedure produced benefits, they were in the process and not the product. It was regarded as a necessary routine, to be met with goodwill but without excessive enthusiasm, and with a determination to stop it developing the sharp teeth sought by some.

What lessons should be drawn from this experience? The Cold War was of course a static period compared with what happened afterwards. From 1990

onwards intelligence has had to adapt to new situations and changes of gear far more flexibly than ever before, and customers' requirements might seem to be much more important than before. Nevertheless, the 20th-century weight attached to them should not be the guide for the 21st. This writer's skepticism is explained elsewhere[13] and can only be summarized here. Customers are busy people, not usually given to defining what they don't know. They often have little idea what intelligence might or might not produce. A future American DCI commented that "often the requirement has more to do with the last item that popped into the policy-maker's in-box or some hairbrained idea he concocted while shaving that morning."[14] They tend to be short-termists; intelligence should not stake too much on their forecasts of what their successors will ask for. It has to take longer views, and make investments accordingly.

Intelligence is also like other kinds of knowledge industry—research and development, for example—in not lending itself well to top-down central planning. Its good practitioners are opportunists. What they do against any target should be a multiple of feasibility and potential value—they should not do anything if the answer to either is zero. But operational feasibility looms larger than for more conventional information producers. Intelligence needs customers' ideas about what they want—including the hairbrained and "blue-sky" ones—and should seek every opportunity for dialogue with them, but stimulation usually comes better from developing customers' feedback on the intelligence they receive than from taking requirements as the starting point.

This takes us back to the market analogy with producers and customers. Intelligence's professionalism is grounded in production standards—seeking to be right—but is wider. The intelligence officer is an information entrepreneur, skilled in engaging individual customers, evaluating its product with them, ascertaining what gaps it leaves unfilled, and feeding the conclusions back into the production machine. Market research and selling are part of the core skills. The analogy with the market is a good one, better than a picture of intelligence in a requirements-driven command economy; but the producer-customer market does not have a perfect balance between supply and demand. Customers have more important things to worry about. Intelligence itself has to supply the dynamic and has the most powerful incentive to do so: Ultimately it goes out of business if customers cease to want its product, whereas customers are normally less dependent. The intelligence-customer relationship is much more "producer-push" than the "customer-pull" implied if requirements are seen as the driving force. The requirements-driven approach reviewed here has the danger of being too mechanistic.

The same criticism might be also applied to the command-driven intelligence cycle as developed in the same period; yet on this there is the puzzle that it retains the confidence of the military and indeed is now more widely seen as the intelligence paradigm. It may be that war is unrivaled in making commanders intelligence-conscious and intelligence-educated to degrees not found in peacetime, except perhaps in counterterrorism. Or perhaps the cycle should be revisited

as a training metaphor, rather than a description of real life, and its emphasis on the commander revised. Other military doctrine now emphasizes subordinates' initiative through "mission command," and perhaps this should be brought to the cycle's exegesis. The problem here may be that those looking at intelligence as a whole just do not know enough about the cycle in recent military experience. Despite battlefield intelligence's modern importance, we lack published accounts of its dynamics in practice.

So there has to be this qualification. But despite this, the lesson from the period considered here can be suggested with some confidence. Requirements as developed in the Cold War served admirable purposes for broad direction, strategy, and legitimacy. Attempts to develop them further had mixed success. It is fortunate that individual agencies' influence in the collegial British system meant that ideas of developing them in ambitious management systems never got off the ground. In all, they did some good and not much harm.

The regret is that they presented a simple, rather seductive approach to understanding intelligence or controlling it. Those dealing with intelligence from outside saw too much promise in it, in years in which there were already too many other nostrums about effectiveness in the public service. Those brought up on the inside were realistic and cautious, but allowed it to absorb effort that might have been used more profitably.

The British community actually needed more central authority than it had. Throughout the period under review, and until quite recently, the need for some authority of this kind was half-recognized, but there was great uncertainty about its purpose. The result for the community was what the Committee of Parliamentarians described as a hole in the center. Supervision of "Requirements" seemed a comprehensible point of entry, but hindsight suggests that it was too narrow. The community needed something more comprehensive, yet more subtle: bound up with the attributes of leadership, rather than a management system.

The recently retired very senior member of the Cabinet Office who had occupied the revised post of Security and Intelligence Coordinator gave a fresh definition of that role at intelligence's center. It was the conviction of "his personal responsibility for intelligence's professional health": a notable statement. It is to be hoped that attention to customer requirements will be handled as part of this more encompassing view of managing intelligence, and not as a short cut.

NOTES

I am grateful for comments and suggestions to John Morrison and Philip Davies. For requirements in SIS I have drawn extensively on the latter's *MI6 and the Machinery of Spying* and other publications.

1. Dictionary definition, *Longman's,* 1984.

2. Both quotations from Philip H. J. Davies, *MI6 and the Machinery of Spying* (London: Frank Cass, 2004), p. 50.

3. Philip H. J. Davies, "A Critical Look at Britain's Spy Machinery," *Studies in Intelligence* 49 (2005), p. 44.

4. Ibid., p. 43.

5. Davies, *MI6 and the Machinery of Spying*, p. 156.

6. Keith Jeffrey, "The Government Code and Cypher School: A Memorandum by Lord Curzon," *Intelligence and National Security* 1 (September 1986), p. 455.

7. F. H. Hinsley with E. E. Thomas, C. F. G. Ransom, and R. C. Knight, *British Intelligence in the Second World War, Vol. 3* (London: H.M. Stationary Office, 1984), pp. 459–60.

8. F. H. Hinsley, *British Intelligence in the Second World War,* abridged edition (London: H.M. Stationary Office, 1993), p. 117.

9. *National Intelligence Machinery* (Norwich, U.K.: H.M. Stationary Office, 2005), p. 24.

10. Air Chief Marshal Sir Douglas Evill, *Review of Intelligence Organizations, 1947*, Misc/P 4781, November 6, 1947, CAB 163/7, National Archives, United Kingdom.

11. Discussed and reprinted in Richard Aldrich and Michael Coleman, "The Cold War, the JIC and British Intelligence, 1948," *Intelligence and National Security* 4 (July 1989).

12. Michael Herman, *Intelligence Services in the Information Age* (London: Frank Cass, 2001), p. 119.

13. Herman, *Intelligence Power in Peace and War*, pp. 283–96.

14. Quoted in ibid., p. 289.

10

GLOBAL ECONOMIC ESPIONAGE

An Ancient Art, Now a Science

MINH A. LUONG

Imitation is the sincerest form of flattery. Others call it economic espionage.

ONE OF THE BASIC MOTIVATIONS THAT DRIVES innovation is the reward from developing an invention, business process, or product. The steady advancement of technology through the ages has led to the development of a global economic system that has raised the overall standard of living and promises to address some of humankind's greatest challenges. In order for the global economy to continue to thrive and innovation to continue, the challenge of global economic espionage needs to be successfully addressed.

Economic espionage is the use, or facilitation of, illegal clandestine, coercive, or deceptive means by a foreign government or its surrogates to acquire economic intelligence. Economic espionage activities may include collection of information, or acquisition or theft, of a manufactured item through clandestine means with the intent of using reverse engineering to gain proprietary or classified data.[1] Economic espionage also includes the theft of product designs, marketing plans, proprietary information such as manufacturing techniques, and intellectual property such as computer software applications.

If left unabated, economic espionage, practiced on a global scale, threatens to destroy the incentives to innovate and will eventually reduce the quantity and quality of new ideas and inventions brought to the marketplace and for the benefit of humankind.

GLOBAL ECONOMIC ESPIONAGE: AN ANCIENT PRACTICE

One of the earliest recorded cases of economic espionage comes from the 18th century, with the European acquisition of the manufacturing process of ceramic porcelain that was a closely guarded secret of the Chinese.[2] The Chinese started producing white porcelain china and tableware as early as the 7th century, and trade in porcelain wares with European royalty was robust toward the end of the 13th century. For over four hundred years European traders and luxury goods makers desperately sought the manufacturing secrets of this "white gold" that fetched large sums of money for entire serving sets and place settings. Because the Chinese recognized the tremendous economic value of holding a global monopoly in porcelain manufacturing, the Chinese emperor centralized all porcelain production and relocated all porcelain craftspeople in an industrial city called Kin Te-Chen that closely guarded the materials, manufacturing process, and potters who produced the porcelain goods. Porcelain production was banned in all other parts of China. Despite all attempts of foreigners to infiltrate the city, bribe craftspeople who were familiar with the manufacturing process, or otherwise learn the secrets of making porcelain, ironically, it was a Jesuit missionary named d'Entrecolles who turned out to be one of the world's first industrial spies.

Because he was a priest, d'Entrecolles was thought to be trustworthy and was allowed access to Kin Te-Chen, where he observed the entire manufacturing process. He became friends with the potter families who produced various porcelain goods and, despite the extensive security procedures of the royal Chinese guards, managed to obtain and send to his contacts in Europe a sample of kaolin clay, the raw material used to produce the valued white Chinese porcelain. Of even more value, d'Entrecolles wrote numerous letters explaining in great detail the elaborate production procedures he learned from his visits to Kin Te-Chen. With d'Entrecolles's sample of kaolin and step-by-step description of the production details, a Saxon chemist named Johann Friedrich Böttger began working on a formulation to produce European porcelain. His initial efforts yielded a porcelainlike material but due to the clay found in Germany, his first sets of products were colored red. It was only through chance discovery of a powder used to dust white wigs that Böttger discovered the elusive final key ingredient necessary to produce white porcelain. Like the Chinese, Böttger implemented elaborate security measures to protect the formulation and manufacturing process that he spent years to perfect. But unlike the Chinese, who were able to protect their trade secrets for four centuries, Böttger was able to maintain exclusive production of European porcelain for less than a decade. Because of industrial espionage against Böttger's firm, porcelain was produced all across Europe by the end of the 18th century.

The rise of mercantilism provides another illustrative example of economic espionage. England, with few domestic natural resources and a relatively small population, used its comparative advantage in technology and global trade to

become one of the world's richest countries and controlled a vast empire. The British either colonized or established British-owned trading companies in many resource-rich areas around the globe that produced spices, teas, whale oil, pelts, silk, cotton, and other valuable raw goods. Through importation of raw materials such as cotton and production of finished goods such as bolts of colorful cloth, articles of clothing, and other textile goods, English textile mill owners and, through trade taxes, the English monarchy, grew rich and powerful.

Two of the premier innovations that kept British industrialists at the forefront of global production and profitability were the cotton spinning process, which automated the process of turning raw cotton into uniform-thickness, high-quality thread, and the famous Cartwright loom, which used the power of falling water from streams and rivers to power massive mechanical looms that weaved cotton thread into large swaths of finished cloth. Thousands of bolts of this unsurpassed cloth were produced by British weaving mills on a weekly basis and because of the uniformity of size and high quality of British textile goods, global demand often outstripped production capacity. Because of the mercantile system and the successful application of spinning and weaving technologies, textile production was as much a goldmine for the British as porcelain production was for the Chinese.

Despite the enormous commercial success of the British textile industry, there were numerous warnings about the longevity of the British monopoly on automated cotton spinning and weaving processes. The impressive feats of British industrial spy Thomas Briand in stealing French industrial secrets on behalf of British interests underscored the importance of protecting industrial and trade secrets. The British realized that their higher standard of living, combined with the costs of transporting raw materials to England and shipping finished goods back to customers around the globe, added significant expense to their final production costs. If their technological and production secrets were ever compromised and lost to manufacturers who could produce those same finished goods in their own countries, many British industrialists would go bankrupt or at the very least be forced to compete with manufacturers that were located closer to their customers and enjoyed much lower overall production costs.

After witnessing repeated failures on the part of firms throughout the European continent to protect their own industrial trade secrets, England adopted a different approach to protecting Britain's mercantile system and industrialists who were pillars of the British economy. In 1765 the English Parliament passed a series of laws prohibiting the transfer of "new machines or plans or models" with the aim of preserving England's technological and manufacturing superiority. The law also forbade tradesmen, repairmen, and others knowledgeable in the workings of protected machines from leaving the country. British industrialists were expected to do what they could to protect their own proprietary information and trade secrets, but the British crown used its network of marshals and constables as well as customs inspectors to investigate suspected industrial spies.

It was not long before an American colonist and engineer named Samuel Slater traveled to England and, through working in various British cotton spinning

mills, learned the entire process of the proprietary British system from preparation of raw cotton bales to winding the finished thread onto large shipping spools. Slater had the gift of a photographic memory to which he memorized the blueprints for various spinning machines and their attendant devices. He also committed to memory the various nuances of cotton spinning learned from working at several of England's best cotton spinning mills. Because Slater worked at each mill for only a short time, he was able to stay one step ahead of the British agents who were charged with identifying industrial spies and, through his work at several mills, was able to learn the advantages and shortcomings of each mill's process. This surreptitious journey made Samuel Slater one of the world's foremost experts in cotton spinning as he was able to convince the normally secretive British cotton processors and spinners in succession to hire him to improve their operations.

Slater was a confident man, and his photographic memory served him well on many occasions. But Slater was also a careful engineer and knew that once he left England, there would be no opportunity to return if he forgot a critical detail or part. So for the most detailed spinning machines, he left nothing to chance and carefully reproduced mechanical blueprints onto large canvas cloths. Knowing that he had now come under the suspicion of the British authorities, Slater left England earlier than he had originally planned but had collected nearly everything that he had set out to discover about the cotton and spinning processes. By leaving on a small ocean sloop Slater was able to evade most of the British immigration control officers and agents who were awaiting him near the berths of the larger galleys headed to the New World. His bags were searched, however, by a customs officer just as he boarded his ship and with nothing that constituted a violation of the British technology control laws, Slater was allowed to travel without incident back to the American colonies. Little did the British authorities know that Slater had arranged to have his canvas mechanical drawings rolled up and hidden in one of the horizontal masts of the sloop, which the British customs officer missed during his search of Slater's baggage and the sloop's cargo hold. Upon his return to New England, Slater quickly raised the funds and built the first cotton-thread spinning mill in the American colonies, which helped start the economic rise of the new republic and earned him the title of "Father of American Manufacture."[3]

Samuel Slater's spinning mills started producing cotton thread in significant quantity, but without an indigenous automated and high-volume looming and textile production capability, producing finished textile goods outside of England remained elusive. The British were furious with Slater's illegal transfer of their cotton spinning technology and production methods and, as a result, refused any imports of finished thread from the American colonies. So the hope of producing cotton thread in America and having that thread woven into cloth by machine in Britain was quickly extinguished. Thus, American cloth remained loomed by hand on small, manually operated looms that produced smaller swaths of cloth

that were inferior in quality and quantity to those of the British automated power-loomed cloths.

By the early 1800s the United States had won its independence from England and American textile mills were desperate to successfully compete with their British counterparts. Thus, a renewed effort to learn the secrets of the British power cotton weaving process began in earnest. Previous attempts by other would-be industrial spies who wanted to be the next Samuel Slater failed as the British enhanced their security procedures and enforcement of their technology transfer laws. But the one industrial spy who would succeed where all others had failed previously was also a highly unlikely candidate by the name of Francis Cabot Lowell, a rich and successful Harvard-educated shipping magnate who came from a prominent and cultured Boston family.[4] Because of his extensive business ties with British trading firms and family ties to England that preceded the American Revolutionary War, Lowell was welcomed by the British textile manufacturers not only as a self-made kindred spirit of sorts, but also as a potential customer and business partner with connections all over the globe. He was given extensive tours of the finest weaving mills and any question he asked was answered in great detail by the mill foreman or the owner of the weaving plant himself. For his part, Lowell kept up the ruse by bringing his family with him to England and telling his hosts that he was in poor health and needed an extended vacation that included consultation with England's best physicians. Like Slater, Francis Cabot Lowell possessed a photographic memory but left little to chance: After each visit to a weaving mill, he sketched drawings of the weaving machines he examined and transcribed the conversations that he had with British weaving experts. By the end of Lowell's "health vacation," he had gathered all the information necessary to reproduce a large powered mill and loom back in America. Though the British industrialists never suspected Lowell of stealing their industrial and trade secrets—after all, he was a gentrified, educated global shipping magnate who knew nothing of their business and would never be a threat to them—British customs authorities were far less convinced. Not wanting to risk being discovered as an industrial spy on British soil and endanger his family who was with him, Lowell arranged to have his drawings and notes smuggled out of England separately, although the exact method was never revealed by Lowell. British customs officers searched the Lowell family's bags repeatedly during their journey to the port, but after coming up empty each time, the officers let Lowell and his family depart England with the second and perhaps most important of England's industrial secrets. Upon his return to Massachusetts, Lowell and his brother-in-law started the Boston Manufacturing Company, and after improving on the water-power delivery mechanism and the designs of the weaving looms themselves, Lowell's mills were weaving more than two miles of very high-quality finished cloth per week—a significant improvement in both quality and quantity over the British mills. The American textile industry witnessed steady growth for the next century and was a major engine of the American

economy until the rise of steam power overtook textile production a few decades later.

Because of Samuel Slater and Francis Cabot Lodge's economic espionage, the industrial revolution began with a strong start in the United States and, along with protective tariffs that allowed fledgling domestic industries to take hold and grow, witnessed the meteoric rise of the United States as a major world power. The rise of the American economy allowed greater capital investments and advancements in industrial technology, which has been the mainstay of American economic growth and power. Today the United States is the world's economic giant, but with that distinction come the pressures of globalization and competition that have led to increased economic espionage against U.S. companies. In essence, the cycle has come full circle. In response to a sharp rise in economic espionage against American industrial firms and military contractors, the U.S. Congress passed the Economic Espionage Act of 1996 (EEA), which imposes prison terms up to fifteen years and fines up to $10 million for stealing trade secrets for the use or benefit of anyone other than the owner. Even with the EEA and increased enforcement by the Federal Bureau of Investigation (FBI), economic espionage in the United States continues to grow at an alarming rate. The lessons of the British technology protection acts of 1765 will serve today's American industrialists and political leaders well as they protect their technological advantages against industrial spies from rival countries.

ECONOMIC INTELLIGENCE: BENCHMARKING NATIONAL COMPETITIVENESS

National governments, regardless of form or type, are under increasing pressure to satisfy the needs of their domestic populations and maintain economic stability and growth. Growing populations around the globe expect paying jobs in order to feed, house, and clothe their families; and an educated elite, frequently educated in the best universities in Asia, Western Europe, and the United States, have rising expectations for their own prosperity and well-being. In an increasingly global marketplace, the competitiveness of domestic industries often means the difference between national prosperity and security versus poverty and instability. For all countries, making intelligent investments in the right industries at the right time is a critical part of national economic policy. Economic intelligence gathered from competitor nations is an essential component in making the right investment decisions.

These investment decisions affect different countries depending on their present stage of economic development. For developing countries, accurate economic intelligence helps direct scarce investment funds to industries that show the greatest promise for long-term growth. In the case of developed countries, economic intelligence is used to help support established but aging industries that need to improve their competitive standing against rival firms from other nations

that frequently operate on a lower cost basis. For all nations, capital investment funds at competitive interest rates are a finite resource and managing those funds effectively requires access to accurate, complete, and timely economic intelligence.

ECONOMIC ESPIONAGE: RESEARCH AND DEVELOPMENT AT LITTLE OR NO COST

Countries collecting economic intelligence use those data to compare how their industries are performing relative to those of other countries. Many countries discover that their national industries require significant capital and technological investments in order to become or stay competitive in the global economy. The policy decisions that result from such findings frequently cross the dividing line between economic intelligence and economic espionage. For countries that can afford to raise capital funds to improve their industries, they certainly engage in economic intelligence but tend to avoid engaging in economic espionage to maintain positive relations with larger trading partners and access to overseas investment funds. Yet for countries that cannot afford to pay to improve their industries, they still face the same demographic, economic, and political pressures of other countries but choose to acquire stolen technology and proprietary information to bolster their uncompetitive industries. These countries maintain legitimate businesses and interact in the global economy but choose to supplement their economic growth with benefits from economic espionage.

The National Counterintelligence Executive (NCIX), the U.S. government agency charged with protecting American industry and trade information, noted that "[i]ndividuals from both the private and public sectors in almost 100 countries attempted to illegally acquire US technologies in FY2004."[5] The report also observed that the United States is not the only country that has experienced losses through economic espionage. The People's Republic of China, Russia, and South Korea all reported cases of foreign economic espionage occurring within their borders.[6] Economic espionage is a global phenomenon that occurs at three levels: National governments engage in economic espionage to benefit their national industries and military forces; companies steal intellectual property and trade secrets from competitors and even joint venture partners; and individual data collectors, also known as industrial spies, gain employment at target firms and steal proprietary information and trade secrets. This information is then sold to competitor firms or foreign governments.

As illustrated in the beginning of this chapter, the benefits of engaging in economic espionage have been demonstrated repeatedly. By stealing completed or near-completed product plans, a competitor can produce and market a copy of the product without incurring the normal research and development costs of bringing that product to market. For industries with high research and development costs—such as pharmaceutics, biotechnology, computer hardware and

software, and military equipment—theft of even a single high-investment product can be enormous. To make matters worse for the original developer, if products derived from stolen proprietary data are manufactured in a country with lower production costs, the original developers may find themselves in an uncompetitive position, even though they developed the product in the first place. Firms that manufacture products derived from stolen proprietary data frequently do not market them in the country or region where the product plans were acquired. This tactic reduces the likelihood of detection by the firms that originally developed the products.

Estimating the losses from global economic espionage is very difficult, if not impossible, due to the fact that some firms do not discover that their product plans or intellectual property have been compromised for months or even years after the initial loss. Many companies never learn that they have incurred a loss from industrial espionage and assume that their reduced market share or lack of success in the market is due to other business factors. Some firms that discover that they have been victims of industrial espionage make a business decision not to report the loss to the authorities for fear of negative publicity, loss of customer confidence, or even a drop in their stock prices.[7] The culture of silence among firms suffering losses from economic espionage has hampered efforts to uncover how modern industrial spies operate and how to develop more effective protective measures.

ECONOMIC INTELLIGENCE AND ESPIONAGE ON THE RISE

Virtually every national intelligence service gathers some form of economic intelligence. Some use economic data to keep national leadership updated on global trends, but most countries with significant economic assets and industrial capacity use their intelligence services in a more proactive way: Intelligence services are increasingly tasked with actively helping domestic firms win business overseas and with collecting valuable industrial secrets to help their own national industries. Some intelligence research firms and think tanks estimate that some of the world's most active intelligence agencies spend between a quarter to a third of their entire intelligence budgets on collecting economic data and industrial trade secrets.[8] The phenomenon of globalization, combined with lowering or eliminating protective tariffs, has greatly increased competition among industrialized nations with rapidly growing developing countries providing even more pressure with their lower wages and production costs.

To keep current with an ever-changing global marketplace, the world's major economic powers have greatly expanded their economic intelligence capabilities since the 1990s. As competitiveness in European markets heated up through the 1980s and into the 1990s, the British Parliament passed the British Intelligence Services Act of 1994, which expanded the scope of its Secret

Intelligence Service (SAS), also known as MI6, to include areas relevant to "the interests of the economic well-being of the United Kingdom."[9] In March 1994 the French government authorized its intelligence services to expand operations into collecting economic and industrial intelligence. Moreover, the following year the French government established the Committee for Economic Competitiveness and Security, which focused on protecting economic secrets and set up an economic intelligence office in the French Foreign Trade office.[10] The People's Republic of China (PRC), also frequently cited as a major collector of economic intelligence and a leading practitioner of economic espionage, operates mainly through the Ministry of State Security (MSS) and the People's Liberation Army, General Staff Department, Second Department (also known as the Military Intelligence Department), coordinating a vast and enhanced overseas collection effort.[11] In the United States the Central Intelligence Agency (CIA) has maintained a large economic intelligence analysis capability since the end of World War II that was enhanced significantly during the Cold War,[12] but that capability was further expanded as the National Security Agency (NSA) upgraded its signals intelligence collection capacity through its ECHELON system, which reportedly is capable of intercepting millions of electronic messages per hour.[13] In the late 1990s, the European Parliament accused the United States, Great Britain, Australia, and New Zealand of using the ECHELON system to gather economic and commercial intelligence against many European countries and their industries.[14] The Science and Technology Options Assessment Panel of the European Parliament (STOA) released several reports on the ECHELON system, culminating in a final report released in 2001. That same year, U.S. Presidential Decision Directive (PDD) 75 on counterintelligence was released, and the directive created a new office, the National Counterintelligence Executive (NCIX), responsible for protecting American economic and industrial interests.[15] In 2003 Japan established the Secretariat of Intellectual Property Strategy Headquarters, tasked with protecting Japan's technological advantages, which is chaired by the prime minister.[16]

Economic espionage has even become a formal academic and professional discipline. France, which has been cited by numerous sources as one of the largest collectors of economic intelligence and foremost practitioners of economic espionage, opened the *Ecole de Guerre Economique* (EGE), or School of Economic Warfare, in 1997.[17] The EGE's mission statement emphasizes "offensive strategy." It trains students in a wide range of intelligence disciplines and awards degrees in economic intelligence, including a doctorate. In the United States there are an increasing number of universities that offer intelligence and national security degrees, some of which specialize in industrial and technological security.

Countries use economic intelligence to assess the state of their own national industries, measure the competitiveness of industries in other countries, and inform policy makers and industry leaders about which domestic industries are in need of further investment or reorganization. Nations that engage in economic espionage do so to improve or maintain the competitiveness of their own national

industries by lowering or eliminating associated research and development costs by illegally appropriating advanced technology and other proprietary information to bring products and services to market at lower cost and frequently faster than if they were developed indigenously.

TYPES OF INDUSTRIES TARGETED

Economic espionage collectors have concentrated their efforts against a number of specific industries due to their value in promoting economic growth and global competitiveness. In the commercial sector, these include agriculture, biotechnology, chemical, computer technology, fiber optics, medical devices, pharmaceuticals, robotics, and telecommunications.[18] Commercial sector industries all play a role in fostering economic growth. For countries that cannot afford to purchase large quantities of expensive pharmaceutical therapies for their populations, scientists reverse-engineer or discover through research in U.S. or European patent offices the formulations. With the correct formulas, domestic pharmaceutical manufacturers can produce the same drugs for a mere fraction of the price charged by the patent-holding developer. Because there is a significant up-front research cost in identifying a promising compound and developing it into an effective therapy, the pharmaceutical industry has been particularly vulnerable to economic espionage. Commentators who have justified economic espionage in this area or defend ignoring patents for certain drugs argue that it is unethical to deny people needed medicine simply because they cannot afford to pay the price set by the patent holder. Pharmaceutical companies have countered that they have offered to provide drugs at cost or even for free, but countries have their own interest in protecting their own pharmaceutical companies.

In countries where domestic food production has leveled off or has dropped, purchasing agricultural technology and materials has proven to be a costly endeavor. Through industrial espionage, acquiring countries can obtain agricultural technology and the formulations to produce fertilizers and pesticides at a much lower cost, provided that they have the necessary domestic manufacturing capability and access to required raw materials. An important point to note here is that although copy-cat equipment and chemicals derived from economic espionage may not perform as well as products manufactured from their original makers, that issue is not the primary concern. The key factor is whether the copy-cat products are better than no products at all or are better than antiquated products currently in use. Given the low cost/high payoff of acquiring technology and products through economic espionage, the improvements are worth the expense.

With respect to military technologies, many countries use economic espionage to improve the capabilities of their military forces as well as to improve the competitiveness of their arms industries. Targeted military industries include aeronautics, armaments, energetic materials, chemical and biological systems,

guidance and navigation systems, information systems, manufacturing and fabrication, marine systems, sensors and lasers, and space system technologies.[19] Countries that engage in economic espionage to collect military and dual-use technologies are frequently trading partners but are restricted from receiving military-grade technologies due to national security export restrictions. Countries with the most advanced military technology and greatest number of export restrictions include the NATO countries of Western Europe and the United States. The investments required to maintain military advantage of potential enemies are significant, running into the billions of dollars in research, development, and deployment costs. Compromised technology losses through economic espionage put these investments at significant risk.

ECONOMIC INTELLIGENCE AND ESPIONAGE COLLECTION METHODS

With the advent of the Internet, conducting basic economic intelligence research is relatively simple. Many governments make their economic data available on the Internet, and government ministries and agencies regularly make data available to international lenders such as the World Bank, International Monetary Fund, and regional development banks as well as private international lenders. When government-supplied data are neither available nor accurate, estimated data are available from investment firms, university research centers, and organizations that specialize in selling economic research to business and governmental clients.[20]

For collectors of economic intelligence, there is a significant difference in operating between open and closed economic systems.[21] In open economic systems, obtaining economic intelligence is relatively easy and utilizes tools not unfamiliar to a stock investor. Government economic reports and company quarterly and annual disclosures make up the foundation of any country analysis. This information can be supplemented and cross-verified by private data and analysis from research firms and investment companies. On-site visits of companies and manufacturing plants are possible if arranged in advance. Even open source analysis of media reports and academic and trade journals provides rich streams of economic data. In closed economic systems, the economic intelligence collection task becomes more challenging. Harassment from law enforcement officials and state security officers hampers collection activity. Government reports and company disclosures are frequently inaccurate, incomplete, misleading, or simply unavailable.[22] Travel restrictions within the country and the need for special permits encumber collection efforts. When contacted for interviews, company officials grow suspicious of any foreigners or persons asking for company data.

For countries with significant national technical means such as satellites and communications interception capabilities, a new dimension of economic data is

available. Satellite imagery and analysis can help produce accurate agricultural yield estimates, projections of industrial output, even mortality rates. Interception of phone calls, Internet messages, fax transmissions, and other communications can be used to verify or confirm intelligence findings. Finally, economic intelligence sources can include businesspeople, academics, and researchers who live in or visit targeted countries. Intelligence services around the world utilize these types of human sources and though some services prefer to debrief citizens who have returned from abroad, others provide a list of targets beforehand so that citizens can exploit any opportunity they encounter.

For economic espionage collectors, the method of operation can vary significantly. Because of their open economic systems, countries engaging in economic espionage frequently establish front companies in Europe and the United States from which to base their operations. These firms operate like domestic companies, and their foreign ownership ties are either not disclosed or are hidden. For the past decade, acquisition of sensitive commercial, military, and dual-use technologies has been at the top of the target list for economic rivals of the European Union and the United States. These front companies attempt to purchase restricted technology and illegally transfer it out of the country. In other instances, these firms form joint venture partnerships with companies who have developed sensitive technologies and the foreign joint venture partner transfers the proprietary information to a third party in violation of the joint venture agreement. Another popular collection method is to arrange an on-site visit where the targeted technology or products are produced. Though the information exchange is supposed to be bidirectional and mutually beneficial, there have been reported incidents of foreign experts entering restricted areas, photographing sensitive areas, and discussing matters and asking questions that are outside the agreed list of topics.[23] Some countries utilize their student and academic connections in targeted countries, recruiting them to serve as intermediaries or even collectors at academic conferences, university laboratories and libraries, industry meetings, and trade shows. One potential area of concern for significant economic espionage losses is through compromised computer systems. An industrial espionage collector, working within a targeted firm with access to the company's computer system, can download and collect computer files containing critical proprietary data. With the advent of high-capacity, low-cost storage devices such as small hard drives and thumb-sized memory sticks, gigabytes of information can be stolen in minutes and detection is virtually impossible.

As companies expand their operations to other countries, computer networks that support overseas operations are vulnerable to attack from a number of sources. If a firm has a presence in a country with an aggressive intelligence agency, that firm is far more vulnerable to penetration because the intelligence agency is more likely to have control of or influence over the local telecommunication system, power grid, even the construction company that built the structure. Intelligence agencies have even planted eavesdropping devices in the facilities of foreign firms.

ECONOMIC ESPIONAGE: DESTROYING INNOVATION AND INVESTMENT

Economic espionage can affect any country's economy regardless of its state of development. In fact, there are countries that benefit from economic espionage and yet are victims of it at the same time. But the dangers to the international trade system from economic espionage are becoming increasingly clear, and this phenomenon affects nearly every level of a nation's economy.

As economic espionage grows in frequency and scale, knowledge that inventions are regularly stolen greatly reduces or even destroys the normal incentives to innovate. Inventors have been deterred from developing products and bringing them to market for fear of having their life's work and investment stolen. Bankers are increasingly leery of making business loans to firms whose products are at risk from industrial espionage. Investors may be discouraged from making investments in companies operating in foreign countries or whose bottom line may be negatively affected by losses from economic espionage. And joint ventures, hailed by many business scholars as a way of linking the developing and developed worlds to create mutually beneficial results, are fraught with dangers of one partner stealing from the other. Officials in countries that engage in economic espionage as national policy defend their practice by saying that their best minds study in highly industrialized nations but never return to help their native country, so stealing technologies and other industrial trade secrets is a way of equalizing for the potential loss of these educated citizens. The "brain drain" effect is difficult to quantify, but it does provide a rationale for engaging in economic espionage.[24]

These types of risks lead to reduced business efficiencies. The risk from economic espionage has deterred companies from entering promising markets due to weak intellectual property protections and risk of economic espionage. The additional expense for enhanced security increases overhead costs and reduces workplace efficiencies as more time is spent on maintaining security measures. Economic espionage has even led to discrimination in the workplace because certain nationalities and ethnicities are associated with industrial espionage.

THE COUNTERINTELLIGENCE CHALLENGE FOR GOVERNMENTS

Some of the largest targets of economic espionage such as the United States have enacted laws punishing economic espionage collectors. For example, in 1996 the United States passed the Economic Espionage Act (EEA), which punishes firms and individuals who steal or transfer trade secrets with prison terms of up to fifteen years and monetary fines up to US$10 million.[25] In 2002 the U.S. Attorney General strengthened the EEA by giving federal prosecutors more latitude in interpreting violations of the Act. In 2005 the United States adopted a new national counterintelligence strategy that signals a change in approach in

addressing economic espionage. The new strategy shifts counterintelligence efforts from a reactive to proactive approach with more emphasis on protecting sensitive technologies. Law enforcement agencies such as the Federal Bureau of Investigation will devote more resources to defeat foreign intelligence operations within U.S. borders. The new strategy also promises to "ensure a level economic playing field for US businesses and industry." Whether that means that U.S. intelligence agencies will be tasked to directly assist individual companies or industries is unclear, but so far the official U.S. government position is that the U.S. intelligence community does not offer assistance to specific companies or firms.

Countries can and should take a more aggressive approach in combating industrial espionage. The primary goal should be to create awareness of the dangers of economic espionage in their business communities. Another top priority should be to train police officers, investigators, and prosecutors about industrial and economic espionage and how to interpret those laws. Customs officers and technology export control officers should work closer with the intelligence and law enforcement agencies to coordinate their enforcement efforts, and governments should work harder to convince companies that should they suffer losses from industrial or economic espionage, they should report the loss to law enforcement and assist prosecutors in the case.

Overall, the counterintelligence challenge is to discourage economic espionage activity while maintaining the integrity and health of a robust international trading system. Governments can work together to establish mutually acceptable intellectual property and patent conventions with the agreement to enforce them uniformly regardless if the violator is from their country or another country. One forum could be the World Trade Organization, which has attempted to create and enforce intellectual property conventions.

PROTECTING PRIVATE FIRMS FROM ECONOMIC ESPIONAGE

Companies need to be more aware of the dangers of economic espionage and take active measures to protect their proprietary information and inventions. This includes training all employees and executives about economic espionage and which procedures to follow. Individuals should take responsibility if they encounter acts of industrial espionage in their firms by reporting incidents to their firm's security officer and law enforcement.[26] Most firms do not realize that economic espionage is an enterprise-level threat. Prevention of economic espionage is the best solution for any firm's long-term financial health, but effective responses to industrial spying require that all employees are trained and prepared to challenge anyone who exhibits behaviors of an industrial spy.

Employees who participate in or speak at industry conferences or academic symposia should be aware that foreign governments and rival firms target

individual experts for specialized knowledge. Collection methods include asking questions during casual conversations, dinner meetings in which more information can be obtained, and requests for previous articles or conference papers—or even working papers in progress. Invitations to deliver guest lectures and presentations, especially overseas, should be carefully considered for industrial espionage potential.

The company computer network is subject to compromise from within the company and from outside hacker attacks. Companies should perform regular security audits of computer file access logs and store critical information on servers with higher grade security. Remote access should be granted only to employees with a bona fide need, and additional security measures beyond passwords should be required. After an employee leaves the company, that person's company identification card should be returned and all computer access codes should be deactivated.

Executives traveling with laptop computers containing important company documents, marketing or product plans, budgets, client lists, and other information valuable to a competitor or foreign government should be especially careful. Laptop computers are frequently stolen and the information stored on the hard drive compromised. If industrial spies have access to an executive's hotel room, the hard drive can be copied when the owner is out of the room. Wireless Internet connections, while convenient, provide minimal security and industrial spies are able to capture transferred files and access passwords. One of the biggest vulnerabilities is the potential for industrial spies to load a monitoring program onto a firm's or executive's computer that sends screenshots and keystroke logs via the Internet. Data that is displayed on the screen and typed on the keyboard can be sent anywhere in the world that the industrial spy designates.

Companies should consider their security measures the first line of defense against industrial spies and economic espionage collectors. Too often executives rely on patent protections, joint venture partnerships, noncompetition agreements, and the goodwill of employees and business partners to protect the crown jewels of the company. Other executives assume that legal proceedings will provide an adequate remedy should the company fall victim to economic espionage. The unfortunate reality, however, is that most firms never discover that their proprietary data has been compromised and that foreign intelligence agencies and industrial spies are far beyond the reach of their country's law enforcement and legal system. The competitive environment of today's global economy dictates a much more self-reliant, proactive approach to securing intellectual property and proprietary information.

CONCLUSION

Economic espionage is an ancient practice that has evolved into a sophisticated science. Rarely practiced by individuals working alone anymore, economic

espionage is now practiced by national governments, multinational firms, and groups of sophisticated industrial espionage professionals. Industrial and economic espionage has been growing in frequency and scope, and there is no current evidence that the current trend will change significantly. Several countries in particular are known for their economic espionage activities and, because of the high stakes in today's global economy, they run the risk of having trading partners and political allies turn against them. History is replete with examples and object lessons of economic espionage, and we would be wise to learn from past experience.

If continued development of new technologies and innovations is part of the future of the global economy, then business people and entrepreneurs will need to work harder to protect their inventions, companies will need to work harder to create secure workplaces and select trusted business partners, governments will need to work harder to protect their own economies and industries, and the global community will need to work harder to address the root causes of economic espionage. The challenges of the new millennia will require an unprecedented level of innovation and creativity. The threat posed by widespread economic espionage undermines the core motivation for turning ideas into innovations: that an inventor, company, or country can be rewarded for their innovations without fear of having that work stolen. If the global community can restore the incentives to innovate and raise the disincentives for engaging in economic espionage, then the global economy has a better chance of fulfilling its promise with innovations that will benefit every region around the world.

NOTES

1. Interagency OPSEC Support Staff, "Economic Intelligence Collection Directed Against the United States," *Operations Security Intelligence Threat Handbook* (1996), available at http://www.fas.org/irp/nsa/ioss/threat96/part05.htm.

2. A brief description of Europe's success in acquiring the secrets of manufacturing Chinese-style porcelain can be found on the NBH (National Security Office of the Republic of Hungary) website at http://www.nbh.hu/english/bmenu94.htm.

3. For a complete history of the theft of ideas and inventions, see Pat Choate, *Hot Property: The Stealing of Ideas in an Age of Globalization* (New York: Knopf, 2005).

4. For a complete treatise on Francis Cabot Lowell's exploits and analysis of current-day economic espionage, see John Fialka, *War by Other Means: Economic Espionage in America* (New York: Norton, 1997).

5. The Key Collectors, National Counterintelligence Executive Annual Report, 2004, p. 3, available at http://www.ncix.gov/publications/reports_speeches/reports/fecie_all/Index_fecie.html.

6. Appendix A, National Counterintelligence Executive Annual Report, 2004, p. 15, available at http://www.ncix.gov/publications/reports_speeches/reports/fecie_all/Index_fecie.html.

7. Ibid., p. x.

8. For example, the Federation of American Scientists (FAS) maintains websites dedicated to the world's intelligence and security agencies, including estimated budgets and their activities. See http://www.fas.org/irp/world/index.html.

9. Controller of the HMSO, the Queen's Printer of Acts of Parliament, Intelligence Services Act of 1994. See http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940013_en_2.htm.

10. B. Raman, "Economic Intelligence," South Asia Analysis Group Papers, February 1999, available at http://www.saag.org/papers/paper50.html.

11. Nicholas Eftimiades, "Chinese Intelligence Operations," statement before the Joint Economic Committee, U.S. Congress, May 20, 1998.

12. By 1951 the National Security Council directed the CIA to determine the overall requirements for the collection and management of "foreign economic intelligence." See Philip Zelikow, "American Economic Intelligence," in *Eternal Vigilance? 50 Years of the CIA,* eds. Rhodri Jeffreys-Jones and Christopher Andrew (London: Frank Cass, 1997), p. 166.

13. The actual capabilities of the NSA's ECHELON system have been subject to intense debate. The Federation of American Scientists (FAS) maintains an ECHELON information website containing various reports on ECHELON, including those of the European Parliament Temporary Committee on the ECHELON Interception System. See http://www.fas.org/irp/program/process/echelon.htm.

14. The Final Report of the European Parliament Temporary Committee on the ECHELON Interception System is no longer available on the European Parliament website, but FAS has a PDF copy available at http://www.fas.org/irp/program/process/rapport_echelon_en.pdf.

15. National Counterintelligence Executive, History of Counterintelligence, undated. See http://www.ncix.gov/history/CIReaderPlain/Vol4Chap4.pdf.

16. For the English-language version of the Japanese Secretariat of Intellectual Property Strategic Headquarters website, see http://www.ipr.go.jp/e_materials.html.

17. See http://www.ege.fr/.

18. See Minh A. Luong, "Espionage: A Real Threat," *Optimize* (October 2003), available at http://www.optimizemag.com/issue/024/security.htm.

19. Ibid.

20. There has been a steady increase in firms that conduct country-specific and specialized economic research. One of the best known is the Economist Intelligence Unit, which produces reports covering political and economic issues on over 200 countries. See http://eiu.com/.

21. For the purposes of this discussion, an *open economic system* is defined as an economic system that promotes transparent and accurate financial and operations reporting. A *closed economic system* is defined as an economic system in which financial and operations reporting is restricted, secret, or distorted as to become inaccurate. Closed economic systems also tend to be heavily influenced or controlled by the government.

22. Field researchers have discovered that economic reporting in closed economies is heavily influenced by political concerns or to mask inefficiencies or corruption.

23. National Counterintelligence Executive Annual Report, 2004, p. 6, available at http://www.ncix.gov/publications/reports_speeches/reports/fecie_all/Index_fecie.html.

24. This point is discussed briefly in John J. Fialka's *War by Other Means: Economic Espionage in America* (New York: Norton, 1997).

25. For the text of the EEA and other resources, visit the U.S. Department of Justice EEA resource website at http://www.cybercrime.gov/ipmanual/08ipma.htm.

26. Many acts of industrial espionage are caught by administrative assistants and support staff who stop and challenge individuals who search trash and recycling bins, who attempt to access computer equipment outside their normal work area, and who access sensitive company files without authorization.

11

THE POLITICS OF INTELLIGENCE POST-MORTEMS

MAX M. HOLLAND

AT LEAST FOURTEEN SEPARATE INVESTIGATIONS, by one count, have been conducted since 2001 into real and/or alleged failures by the U.S. intelligence community. These inquiries have ranged from quiet, internal probes mounted by inspectors general or consultants, to highly publicized congressional inquiries replete with partisan edges, to semi-public inquests conducted by presidentially sanctioned, bipartisan commissions. By early 2004, so many different bodies had claimed a piece of the post-mortem pie that Senator Pat Roberts (R-Kansas), chairman of the Select Committee on Intelligence, was moved to remark, "Is there anybody left down at [Central Intelligence Agency headquarters in] Langley doing their job? I think the only thing lacking is an independent commission to investigate all the independent commissions and investigations."[1]

Roberts's observation may have been tongue-in-cheek, but he actually suggested an interesting and neglected question: How objective, and useful, are intelligence post-mortems? Such analyses, particularly when produced by Congress or blue-ribbon commissions, are usually accorded an exalted status from the moment they are released. Frequently, they are considered a reliable account of what went wrong and why, if not an authoritative and objective one.

But should post-mortems be embraced so often at face value?[2] Or are they subject to personal/political/institutional pulls and tugs that can easily distort their findings? Admittedly, it can be argued that every congressional post-mortem is congenitally partisan, and that bipartisan special commissions are also not immune from political considerations, although their politics may be much more subtle.[3] In addition, such efforts are invariably confronted with the not insubstantial problem of gaining access to all the relevant information residing in the Executive Branch. Consequently, any baseline examination of this question

would seem to require a series of post-mortems about a single episode, all of them conducted outside the public eye to minimize the influence of partisan politics, and with unfettered or at least roughly equal access to the pertinent information. Ideally, each of these post-mortems would also have been conducted by a different individual or panel, and intended for divergent audiences, in order to gauge the influence, if any, of these variables.

A series of post-mortems on the Cuban missile crisis, all conducted at various altitudes of the U.S. government in 1962–63, fits these parameters. The four post-mortems have actually received scant notice despite the vast literature about the October 1962 crisis.[4] The inattention probably stems from the fact that all of the post-mortems were undertaken in secret and were highly classified initially. Three have gradually become available since 1992, although one post-mortem remains inexplicably classified.[5]

What is striking was how the four ex post facto analyses varied in their findings and conclusions regarding the performance of the intelligence community in the run-up to the missile crisis, notwithstanding the sameness of the facts at issue.[6] The post-mortems were subject to extraneous influences that distorted their findings and even their presentation of fact. It mattered greatly who wrote the post-mortem, when, and for whom. The government's seeming inability to be consistently objective in 1962–63, in turn, is a sobering thought during a period when looking backwards is a growth industry.

CRITICAL ISSUES AFTER OCTOBER 1962

The public terms of the settlement all but guaranteed that the missile crisis would be perceived as a manifest success for the Kennedy administration and the intelligence community—one that the CIA sorely needed, still laboring, as it was, under the Bay of Pigs millstone.[7] Yet the Agency's margin of success was actually very narrow. Once all the facts were in, the missile crisis could be fairly called a "near-failure of American intelligence . . . of the first magnitude," as one scholar put it in 1974.[8] All intelligence estimates prepared prior to mid-October predicted that the Soviets were not likely to implant surface-to-surface missiles (SSMs) on Cuban soil. Of equal if not greater moment, the first hard evidence of the deployment was not in hand until October 15, more than a month after the SSMs had arrived and just days before the CIA would deem some of them operational.[9] That meant Soviet Premier Nikita Khrushchev had come surprisingly and uncomfortably close to accomplishing his strategic surprise.

Three shortcomings thus warranted close examination. One was estimative, namely, the months-long miscalculation of Moscow's intentions. Another was analytical, or the seeming failure to grasp indicators that suggested something other than a defensive build-up was taking place. The third shortfall concerned collection, or the seeming delay in acquiring hard evidence of the missile deployment.[10] These intelligence deficits were hinted at in newspaper stories as

early as October 31, just after the acute phase of the crisis peaked. One immediate question, as an article in the *New York Times* put it, was whether intelligence "estimates [had been] tailored to fit top policy beliefs," or if administration officials had "reject[ed accurate] estimates as erroneous."[11] Another outstanding question, which would be variously dubbed the "intelligence," "picture," or "photo" gap, concerned why it had taken the administration so long to detect the deployment. "[T]here is general mystification about how the Russians could have built so many missile sites so quickly without warning," the *Times* article observed.

All four post-mortems (and many nonofficial ones) would address these primary questions. There was, however, a dramatic difference in the political consequences attached to these shortcomings. With respect to the misestimates and any analytical deficit, unless it could be shown that the White House had tried to influence the process or ignored evidence presented to it—in particular, the mistaken Special National Intelligence Estimate (SNIE) of September 19, 1962—only the intelligence community, rather than the administration, stood to be criticized.[12] The exact opposite was true with respect to the photo gap. In this case, the administration would surely bear the brunt of criticism, because it was the White House and State Department that had effectively ordered the CIA to attenuate U-2 aerial surveillance in mid-September.[13] Conceivably, the intelligence community might be criticized for acceding too easily to the administration's cautious overflight policy, dictated just as the first surface-to-surface missiles were actually arriving in Cuba. But much of the onus for the fact that "American intelligence . . . went blind for five crucial weeks" was going to fall on policy makers in the Kennedy administration—that is, if all the facts came out.[14]

Although the post-mortems were not exactly unanimous in their findings about the misestimates and analytical shortcomings, those deficits will not be addressed here.[15] For the purposes of this chapter the telling issue—the one that genuinely reveals the limits on and of post-mortems—was the serial treatment of the "photo gap" during the inquests conducted from late 1962 to early 1963. The photo gap represented a genuine political problem for the administration. It left the president vulnerable to the charge that he had been taken in by the Soviets' elaborate campaign of deception, to a point where the administration had even tried to foist a false sense of security onto the country.[16]

THE LEHMAN REPORT

Richard Lehman, a 13-year veteran of the Agency by 1962, held the formal title of assistant for special projects in the Office of Current Intelligence (OCI) at the time of the missile crisis. He had made his mark by successfully developing the President's Intelligence Checklist (PICL, pronounced "pickle") in the spring of 1961, a time when the CIA was particularly anxious to please the president.[17]

Allen Dulles's presentations had been considered somewhat patronizing and shallow, and simultaneously, the White House had felt overwhelmed with redundant and often tedious publications from various arms of the intelligence community.[18] The White House had informed OCI director Huntington Sheldon that his office had to come up with an entirely different way of presenting its information in order to gain the president's confidence.[19] It had fallen to Lehman, working under Sheldon, to write a concise, jargon-free, and reliable summary of everything the intelligence community thought the president should know. To the Agency's great relief, Kennedy responded with enthusiasm to the new document, and the PICL instantly became a CIA fixture, making Lehman's reputation in the process.[20]

On Saturday, October 27, 1962, the very day that would prove to be the turning point in the missile crisis, Russell Jack Smith, Sheldon's successor as OCI director, called Lehman into his office and said John McCone, the director of Central Intelligence (DCI), wanted an analysis of the Agency's performance to date.[21] Although the end of the crisis was seemingly not yet in sight, "McCone wanted to know how we had got[ten] there," Lehman later recalled, "what we [had done] right, what we [had done] wrong, and so on.[22] The timing, in retrospect, was quintessential McCone. With typical foresight, the business tycoon-turned DCI was already anticipating what he might need next. Once the November election passed, McCone fully anticipated the possibility of congressional hearings akin to the Pearl Harbor investigation launched by Congress in 1946.[23]

The DCI "pushed the button" so that Lehman had access to everything he wanted to see, and Lehman's research was aided greatly by the fact that McCone had a habit of "keeping meticulous memoranda for the record" of actions, meetings, and conversations.[24] Within four days Lehman had a manuscript of nearly 100 pages on the events leading up to the missiles' detection, including some long-hand annexes that were "for McCone's eyes only."[25] All told, the OCI officer worked on his report for 2½ weeks, making one revision of his initial draft. The final product was in the same "warm, direct, somewhat Thoreau-like style," that had made the PICL so accessible and successful.[26] The report, like the PICL, was jargon-free and its tone candid.

With respect to the key operational shortcoming, Lehman correctly zeroed in on the events of September 10 as being absolutely "crucial to the record."[27] On that day, an extraordinary meeting had been convened at the White House by McGeorge Bundy, Kennedy's national security adviser, in concert with Secretary of State Dean Rusk. The two men, still smarting over criticism that they had not done enough to protect the president before and during the Bay of Pigs invasion, were anxious to prevent an embarrassing U-2 incident over Cuba now that surface-to-air missiles (SAMs) capable of downing the high-altitude surveillance aircraft were being installed all over the island.[28] Bundy and Rusk were deeply concerned that continuation of intrusive overflights would climax in a fatal incident that would put the president in a double bind: Abroad he would be criticized

for violating sovereign airspace, while at home, conservative critics would claim the incident was a *casus belli* that provided the perfect opportunity to "do something" about the unprecedented Soviet military build-up on the Caribbean island.

Consequently, on September 10, Bundy had asked the members of the Committee on Overhead Reconnaissance (COMOR), the U.S. Intelligence Board (USIB) subcommittee that developed U-2 requirements for presidential approval, to attend a special White House meeting at 5:45 pm. In the absence of McCone, who was vacationing on the French Riviera, and under pressure from Bundy and Rusk, the COMOR agreed to attenuate the thorough, bi-monthly overflights of Cuba that had been the routine since early 1962. The next four U-2 flights would either pass quickly over discrete portions of the island or skirt it altogether. In this manner, the Kennedy administration degraded the one intelligence-gathering tool capable of delivering precisely the kind of dispositive information about possible missile deployments that the White House was insisting upon. Together with delays caused by predictably inclement weather, the net result was a dysfunctional intelligence regime in a dynamic situation.[29]

Lehman's blunt recollection of his post-mortem, forty-one years later, was that President Kennedy had "shot himself in the foot" by attenuating U-2 coverage over Cuba.[30] Needless to say, that was not how the OCI officer characterized his findings in 1962. Insofar as Lehman reached conclusions in a report not initially intended for wide circulation, they were careful and understated—more like observations than conclusions. The report was not exhaustive, but it did reflect the gist of what had happened in the weeks leading up to the discovery of the missile sites.[31] One of the senior officials known to have read the report was Dr. Herbert Scoville Jr., the deputy director of research (DD/R). The paper was an "excellent presentation of the facts insofar as [Scoville] knows them," although the DD/R differed regarding one significant aspect.[32]

Lehman noted, with respect to the photo gap, that the U-2 overflights permitted after September 10 were successful, inasmuch as they established new facets of the military build-up, including the complete pattern of SAM deployments throughout the island. Yet the U-2 missions "did not—and since they were designed to avoid SAM-defended areas, could not—detect the ballistic missile deployments then under way."[33] Lehman also observed, and quite correctly, that responsibility for the cautious overflight policy might not appear to be as clear-cut as it in fact was. Coming away from the September 10 meeting at the White House, COMOR members had understood, in no uncertain terms, that intrusive overflights, if proposed, would not be sanctioned by the Special Group Augmented (SGA) for submission to the president for final approval.[34] Still, the record showed that the president authorized everything the SGA had requested, and technically, the SGA had not turned down any written requests from the COMOR for more intrusive overflights. A critical condition imposed on the overflight regime for five weeks had not actually been captured on paper, and this fact would assume ever-larger significance in succeeding post-mortems.

THE IG (OR EARMAN) REPORT

Several days before Richard Lehman completed his report in mid-November, Jack Earman, the CIA's Inspector General (IG) since May, took up virtually the same task. Earman had been an Army lieutenant colonel prior to joining the Central Intelligence Group, forerunner to the Agency, in 1946. For most of his intelligence career, he had enjoyed a view from the top, serving from 1950 until 1962 as a special assistant to the DCI.[35] Analyzing the performance of the intelligence community prior to the discovery of the missiles would easily be the most important assignment he had undertaken since becoming IG six months earlier.

The reason why McCone asked for two internal post-mortems remains unclear, but there is no doubt that he did. Perhaps after his comparatively informal request to Lehman, McCone wanted a more structured or explicit effort. Inexplicably, Earman's report remains classified. Still, there is one extant, albeit redacted, memo that sheds light on Earman's treatment of the photo gap.

Earman finished a draft of his post-mortem on November 20, about one week after Lehman had put the final touches on his report. With respect to the photo gap, Earman's initial account apparently glossed over this operational deficit entirely, or otherwise treated it in a manner that roused McCone, perhaps by placing too much of the onus on the Agency. The DCI instructed Earman to take another look at the factors behind the decision to attenuate U-2 coverage in September.[36] In response, Earman described, in a November 26 memo, how he intended to incorporate McCone's criticism in a revised account.

> We have been told by several Agency officers that there was a widespread understanding in CIA that overflights of known SAM sites were forbidden by the Special Group [Augmented]. I believe this understanding stemmed from the desires which Secretary Rusk expressed at the 10 September 1962 meeting in Mr. Bundy's office which was not in fact a duly constituted meeting of the Special Group. However, the records do not reveal that CIA pressed for additional missions or changes in coverage of overflights approved for September 1962.[37]

Earman then went on, in the same memo, to recount the history of September overflights in some detail, and recited his new conclusion—one that would not be that different from Lehman's, although Earman's point was not as sharp. The net effect of the "extreme caution" after September 10, he wrote McCone, was that "the period of time during which the western part of Cuba was not covered by aerial photography was greatly lengthened."[38] The precise wording of his finding, Earman wrote, would be "[t]hat extreme caution with regard to U-2 flights following the incidents in Sakhalin and China affected the planning of Cuban reconnaissance overflights during [September]."[39]

Thus, McCone essentially put the Lehman and IG reports into consonance with one another on the reasons for the photo gap.[40] Neither of these internal post-mortems attempted to shift the entire responsibility onto the State

Department and/or White House for the deficit in coverage. More than anything, they were simply candid about the fact that estimative and analytical errors, together with the administration's overweening concern about an international incident, had led to a significant degradation of dispositive intelligence-gathering precisely during the period when the first offensive missiles were being maneuvered into place.

THE USIB (OR DCI'S) REPORT

On November 14, the same day Lehman turned in his report to McCone, Dr. James Killian, chairman of the President's Foreign Intelligence Advisory Board (PFIAB), asked the CIA to produce an "all-source, all-agency" review. [41] Killian requested that this survey of the community's performance include all intelligence activities up until the discovery of offensive missiles on October 14, and for the seven days afterwards, ending with President Kennedy's address to the nation on Cuba. Killian further requested that the post-mortem be submitted in time for the PFIAB's next meeting on December 7, 1962.[42]

The PFIAB, an elite, ostensibly nonpartisan panel established by President Eisenhower in 1956, was composed of experienced U.S. officials currently outside the government, augmented by some of the best scientists in the nation.[43] Its purpose was to advise the president directly on all matters concerning U.S. intelligence, from technical collection to counterintelligence. President Kennedy had all but ignored the advisory panel as an unnecessary, bureaucratic impediment very early in his administration, only to revive it hastily after the Bay of Pigs debacle. Thus, PFIAB's standing as one of the few external overseers of the intelligence community, along with its access to the president, guaranteed that the stakes in the third post-mortem would be very high.

Wearing what he called his "DCI hat," McCone transmitted Killian's request to the USIB the very next day.[44] This interagency body, in existence since 1958, represented the pinnacle of the intelligence community at the time, counting among its principal members the CIA, Defense Intelligence Agency (DIA), National Security Agency (NSA), and the State Department's Bureau of Intelligence and Research (INR).[45] The USIB post-mortem would thus not bear the CIA's imprimatur alone, but represent the coordinated judgment of the intelligence community, just as most of the community had been engaged in the intelligence coverage prior to the missiles' discovery.[46] To prepare the report, the USIB immediately appointed a steering committee composed of McCone and several other USIB principals: Roger Hilsman, director of INR; Lieutenant General Marshall "Pat" Carter, deputy director of the CIA; Lieutenant General Joseph Carroll, director of the DIA; and Lieutenant General Gordon Blake, director of the NSA. Simultaneously, a working group was established inside the CIA to do the actual research, analysis, and drafting of the post-mortem, with each of the principal intelligence agencies permitted to assign one officer to this subcommittee.

McCone's choice for chairman of the working group was Jack Earman, the CIA's IG, who was, of course, six days away from wrapping up his own report.[47] In one sense, this third post-mortem would simply be an extension of the analysis Earman was already deeply engaged in. Yet it also differed in two enormous respects. The USIB post-mortem would be conducted with the active participation of intelligence chiefs and officers with direct stakes in the findings, and these same drafters (apart from Earman) would be, in effect, examining their own performance.

Not surprisingly, perhaps, and unlike the first two internal post-mortems, this study instantly evoked wariness among some of the offices that stood to be closely scrutinized. A day before Killian formally submitted the PFIAB request, Dr. Scoville, the head of the CIA directorate that contained the Office of Special Activities (OSA), which actually operated the CIA's U-2s, made the following announcement to his staff, as recorded by an assistant.

> An inquiry would be made into the intelligence coverage and reporting of the missile build-up in Cuba and [Scoville] said that a post-mortem from the standpoint of how more timely and precise intelligence might have been achieved would be a good idea. His fear was that there might be some buckpassing and he wanted OSA to review carefully all factors leading up to the 14 October date (when missiles were actually discovered), taking into account all requirements, COMOR actions, Special Group actions, weather factors, etc.[48]

Scoville's remark about "buckpassing" was almost certainly a reference to the operational deficit in U-2 coverage. The DD/R was apparently anticipating the distinct possibility that some parties represented on the USIB might be inclined to obfuscate the factors that created the photo gap, if not place the onus for the deficit on the CIA in general and his directorate specifically.

Scoville's concern was shared at other levels, including by James Reber, the COMOR chairman. After experiencing two post-mortems already, Reber had considerable doubt about the "validity of people's memories[,] as they unintentionally embroidered the facts."[49] No one, of course, knew better than Reber how the photo gap had come about; he had attended the extraordinary September 10 meeting at the White House when McGeorge Bundy made the president's wishes directly known.[50] Reber also advised Scoville that the CIA representative on COMOR was "exercised because he felt that COMOR performance in the Cuban situation was not being adequately defended."[51] Reber himself was still sanguine about the USIB post-mortem, probably because Jack Earman was in charge of writing up what was by now a supposedly well-established chronology. Reber had read the IG report to the DCI, which he thought was excellent; parts of this earlier post-mortem might even be incorporated in toto, or so Reber believed.

But a problem with establishing the facts soon surfaced. The officers seconded to the working group had been tasked with making sure that their

respective agencies provided all relevant information, and accordingly, an eight-page questionnaire had been submitted to every IC entity, with responses and documentation due back by November 23. As the questionnaires started to trickle in, however, it became apparent that not everything of import was fully reflected in the written record.[52] Some significant "happenings . . . were not recorded except in memory," because few, if any, officials and officers were as diligent as McCone was in jotting down detailed descriptions of key encounters.[53] And nowhere was this lack of documentation more telling than with respect to the photo gap, as Lehman had been the first to point out. The September 10 decision to degrade overflights was imperfectly reflected in the written record, and the documentation that did exist left the implication that the CIA had not been very exercised by this limitation on overflights imposed from the White House.[54] No one in the CIA seemed to have energetically pressed for additional missions or changes in coverage, according to the written record, until the DCI himself made the case on October 4. Consequently, it could easily be made to appear as if the Agency got exactly the operational coverage that it had asked for.[55]

The relative paucity of contemporary documentation might have been less of a problem but for the predispositions INR Director Roger Hilsman brought to the post-mortem. Hilsman had had a difficult relationship with the Agency from the outset of the Kennedy presidency, and he viewed the post-mortem as nothing less than a crucial engagement in his ongoing war with the CIA. Like many liberals in the administration, he had come into the government believing that the CIA had gotten so powerful during the 1950s that "it was running the foreign policy of the United States."[56] Allen Dulles had been a "de facto Secretary of State," and one of the tasks Hilsman had set for himself was "cutting [the Agency] back in power," and "sav[ing] the [State] Department from the CIA" by reducing the latter's alleged policy-making proclivities and overweening influence.[57] Hilsman regarded the CIA as a mortal rival in the intelligence sphere because the Agency wanted "anything that smack[ed] at all of intelligence interpretation to be theirs."[58] Rank-and-file CIA officers who dealt with Hilsman regarded him as "often wrong, but never in doubt," an able person with a marked propensity for the "perpendicular pronoun" who was always seeking to insert himself in the bureaucratic process.[59] Others pegged the INR director as more of an ambitious sycophant than anything else, interested primarily in ingratiating himself with the Kennedy brothers whenever possible.

One illustration of the antagonistic relationship was an incident that allegedly occurred on October 16, the very day President Kennedy learned of the missiles in Cuba. The scuttlebutt around the Agency that day was that as Hilsman was preparing to see Dean Rusk that morning, the INR director remarked that he was going to have to report a "tremendous failure on the part of U.S. intelligence."[60] When DDCI Marshall Carter called Hilsman and asked him about the reported comment, Hilsman averred that he didn't recall saying anything of the kind—only that he, along with almost everyone else in the administration, did not expect the Soviet deployment.[61]

Coming from his perspective, Hilsman was intent on using his position on the steering committee to scrub the USIB post-mortem for anything that seemed like the CIA patting itself on the back at the expense of the State Department, and the administration in general. This goal was all the more urgent, of course, because only McCone, from among all the president's advisers, had anticipated the emplacement of offensive missiles and distinctly warned Kennedy of that possibility. The aftermath of the crisis thus promised to afford McCone an opportunity to "manipulate [the missile crisis] to his advantage," and strengthen the DCI's and CIA's position within the administration—this, at the very time when Hilsman was intent on "cutting them back in power."[62]

Although contemporaneous documentation about the internal wrangling over the USIB post-mortem is not extant, there is little doubt that extended negotiations over its language took place; that Hilsman was at the center of these disputes; and that much of the contention revolved around how to depict the "extreme caution" that degraded U-2 coverage from September 10 until mid-October, and the consequences that flowed from that policy.[63] Much of the evidence for these inferences comes from McCone's reaction to the first draft of the USIB post-mortem as submitted by Earman in mid-December. Typically, the DCI minced no words in his December 17 response. ". . . your brief treatment [of the September 10 decision] gives me the impression that we are obscuring the fact that there were policy decisions based on concern over . . . a U-2 incident," he wrote Earman.[64] Indeed, the DCI felt the draft did not answer many questions he still had about the pivotal September 10 decision that had been reached in his absence. "I do not have an explanation of this and I'd like to know where this change in procedure came from, by whose order, and under what circumstances," McCone wrote.[65]

The USIB working group went through three drafts before a version was even deemed fit for review by the steering committee on December 5. By that time, it was obvious the report would not be submitted to PFIAB by December 7, as requested by Killian, so the steering committee gave PFIAB an oral progress report on December 6 and 7, after which McCone promised to have a final, coordinated draft in no more than two weeks. It then took a flurry of meetings of both the steering committee and working group before a "final" draft—the sixth—was agreed to on December 23—although three days later, Hilsman expressed reservations yet again.[66] By that time, McGeorge Bundy had gotten wind that the post-mortem was nearing completion, and given his role in attenuating the U-2 coverage, he requested that a copy be delivered immediately to him in Boston, where he was spending the Christmas holiday. Bundy also insisted that no copies be distributed outside of the government until he had had an opportunity to read the politically sensitive document, and that included no copies to the PFIAB.[67] The matter would finally come to an end on January 3, 1963, when the USIB steering committee agreed that no further amendments were necessary and McCone was authorized to inform Killian that the seventh draft of the report was, in fact, the final one. The post-mortem was officially submitted to the PFIAB on January 7.

Apart from McCone's initial reaction, and the arduous negotiations that went into the numerous drafts, the best insight into Hilsman's influence on the USIB process is gained by comparing the USIB post-mortem to his controversial 1967 memoir, *To Move a Nation*.[68] Juxtaposing the two, if nothing else, starkly reveals the not-so-hidden agenda Hilsman brought to USIB deliberations over the post-mortem's language. Hilsman's position was that of loyalty to the administration rather than the facts, with the goal of insulating the administration from criticism for having degraded the one intelligence-gathering tool that was indispensable.

In his memoir Hilsman devoted an entire chapter to the aftermath of the missile crisis, which he entitled "The Intelligence Post-Mortem: Who Erred?" Specifically referring to the USIB report, Hilsman termed it one of "two attempts by insiders to allege that policy [had] interfered with intelligence."[69] McCone instituted the study, Hilsman wrote (incorrectly),

> immediately after the crisis to determine if the missiles would have been discovered sooner if the Secretary of State had not requested on September 10 that the next [U-2] flight be broken up into four separate flights. For a while there was some uneasiness at the possibility of some real alley fighting developing. But it was not difficult to show, first, that any delay caused by making four flights instead of one was negligible; and, second, that there had never been a turndown of any flight that intelligence had asked to be approved, but that on the contrary both the White House and the State Department had actually pushed for more intelligence all along.[70]

In an adjacent passage Hilsman flatly asserted that there was "no evidence of any attempt by the policy-makers to suppress information or to hamper intelligence-gathering activities. No request from the intelligence community to fly a U-2 over Cuba was ever refused."[71]

It was disingenuous to claim, of course, that the September 10 decision had not markedly interfered with the collection of hard intelligence, not to mention dishonest to pretend as if the extraordinary session at the White House had never happened. At the same time, and despite these denials, Hilsman tacitly admitted that there had been some kind of delay in discovering the missile sites. But that, still, was a nonissue, because it was reasonable to believe that the U-2 flight on October 14 "found the missiles at just about the earliest possible date."[72] Ultimately, Hilsman concluded that the discovery of the missiles had to be "marked down as a victory of a very high order" for American intelligence, though "it had also been—in one sense at least—a little lazy."[73]

As but one member of the steering committee, Hilsman could not dictate the USIB post-mortem, much less unilaterally impose his peculiar views about what had happened. Yet when Hilsman's 1967 account and the USIB report are juxtaposed, it seems clear that his preferred conclusions carried the day. The issue of the photo gap—by any measure the most important operational shortcoming in the run-up to the missile crisis—was not even raised until page 69 of the ninety-page post-mortem, when the September 10 "special meeting" was mentioned for

the first time. Jack Earman was apparently able to wring only one concession: that the CIA at least believed the overflight regime had been degraded in mid-September.

> There was a difference of opinion in the 4 October Special Group (Augmented) meeting on whether a restriction had been imposed on overflying known SA-2 sites. Because of the skimpiness of records, it cannot now be discovered whether there was or was not such a restriction. It is clear, however, that the operational elements were under the impression that such a restriction did exist. Evidence of this belief can be found in the reference to such a restriction by the DCI at the 4 October meeting of the Special Group (Augmented).[74]

Besides obfuscating responsibility for attenuation of photo coverage, the USIB post-mortem concluded, almost like Hilsman would four years later, that the photo gap had not mattered even if it existed. "The procedures adopted in September delayed photographic intelligence," stated the USIB report in its conclusionary chapter, "but this delay was not critical, because photography obtained prior to about 17 October would not have been sufficient to warrant action of a type which would require support from Western Hemisphere or NATO allies."[75] In this regard the INR director probably did not have to be so persuasive, as all the USIB members had a vested interest in propagating this conclusion, or something close to it, to anyone outside the immediate intelligence community, even the PFIAB. Not uncoincidentally, perhaps, this position was nearly identical to the administration's public posture, which had been roughly hammered out in the midst of the crisis.[76] This finding was in decided contrast to the Lehman and IG reports, which made no such claim and, indeed, suggested the opposite.[77] Presumably, during the deliberations over the USIB report, Earman probably maintained that the post-mortem would be remiss if it did not somewhere state that the September 10 change in the surveillance regime resulted in a delay of photo coverage. In turn, Hilsman argued vigorously, in all likelihood, for qualifying language that simultaneously rendered this operational deficit meaningless, if it had to be admitted at all. The bottom line was a compromise finding notable for being acceptable to both sides and the administration's public position, rather than the truth of the matter.[78]

Overall, the USIB report, the only coordinated post-mortem that would be produced, was a carefully structured and detailed description of the intelligence accumulated and evaluated on a communitywide basis in the run-up to the missile crisis.[79] It was much more systematic and workmanlike than Lehman's analysis, the tone of which was informal. Its key conclusion, which it shared with its predecessors—no doubt because it was incontrovertible and not controversial—was that the IC's "analytic effort, using a variety of sources, identified each of the major weapons systems introduced into Cuba before the system reached operational capability."[80] But in contrast to the Lehman and IG reports, the USIB report has to be considered as a negotiated (if not compromised) post-mortem, the

product of a hard bargain between competing and conflicted government elements that was, ultimately, not even satisfying to those same elements.[81] The USIB report tried hard to give the appearance of presenting the facts in a plain, unvarnished manner. But whenever a problematic fact reared its head, the language was massaged until the post-mortem was acceptable to vested interests—bureaucratic as well as those of the incumbent administration.

THE PFIAB POST-MORTEM

The USIB report, despite the intense bargaining over the precise language of its findings, was never viewed as an end in itself by PFIAB members, only a starting point. Mindful of their direct access to the Oval Office, a privilege they jealously guarded, the board always intended to gather additional information as necessary and make its own evaluation for submission to the president.[82] From the perspective of PFIAB's nine members, the USIB's coordinated post-mortem was likely to represent a "best foot forward" approach by the intelligence community and its titular head, the DCI, if only because its drafters were examining their own performance.[83] Any and all estimative, analytical, or operational deficits were likely to be downplayed, buried, or rationalized into insignificance.

But PFIAB members were also inclined to be skeptical because relations with John McCone—at least from PFIAB's perspective—were uneasy at best. DCIs, it seemed, tended not to like having an independent board looking over their shoulder, "encroaching on their prerogatives."[84] In this regard, McCone was scarcely different from Allen Dulles. Upon taking over as DCI in November 1961, McCone had allegedly attempted to alter PFIAB's standing so that it reported to him rather than the president. The panel members had not forgotten this alleged "early run" at PFIAB's authority, and relations with the conservative and outspoken DCI were, as a consequence, fairly tense.[85]

McCone's relationships with Dr. Killian and Clark Clifford, the two most important PFIAB members, further complicated matters. A former president of MIT, Killian had had several bruising run-ins with McCone in the late 1950s, while McCone was chairman of the Atomic Energy Commission and Killian was both President Eisenhower's first science advisor and, simultaneously, chairman of both PFIAB and the President's Science Advisory Committee. McCone was of the general opinion that "scientists cause trouble" in the federal government because they tended to inject themselves into political matters rather than sticking to what they knew and were supposed to be do, which was provide the best technical advice.[86] Killian, naturally, took exception to McCone's attitude. After President Kennedy had announced McCone's appointment as the new DCI in September 1961, the *Washington Post* reported that Killian "was so out of sorts over the appointment that he threatened to resign as [PFIAB's] chairman."[87] Although Killian promptly denied the story, it was nonetheless true.[88]

Yet the McCone-Killian relationship wasn't even the most problematic. If McCone could be said to have a true nemesis on the board, it was Clark Clifford, the archetypal Washington lawyer, and a skilled, consummate, and partisan defender of the president's interests, specifically, and the Democratic Party's, in general. Clifford styled himself as having been "present at the creation" of the postwar intelligence community, although he probably exaggerated his role in drafting the legislation that established the CIA.[89] Still, the experience was sufficient for him to consider himself something of an expert on intelligence matters. Moreover, in the wholesale reshuffling of the administration that occurred after the Bay of Pigs debacle, President Kennedy reportedly offered Clifford the DCI's job, only to have Clifford decline the honor of succeeding Allen Dulles.[90] Thus, Clifford operated from a position where he was confident of his expertise and knew he was Kennedy's preferred choice for DCI, and he did not regard the notoriously inflexible McCone as a very good second choice. McCone's standing as a rich Republican businessman who had served Eisenhower and remained close to Richard Nixon, plus McCone's reputation as a "deeply ideological anticommunist," also inclined Clifford to be critical and wary of the DCI.[91] Just as McCone was taking up the reins at the CIA in November 1961, Clifford, at the president's request, had submitted a briefing memo outlining what Clifford thought would be the most important points to keep in mind as Kennedy began the relationship with his new DCI.[92] That only underscored Clifford's sense of having a direct, and perhaps even superior, line of communication with the president.

Clifford apparently agreed to serve on PFIAB after declining the DCI post, once Kennedy reconstituted the board after the Bay of Pigs debacle. Since PFIAB's inception in 1956, its appointees had been selected largely for their scientific knowledge or foreign policy expertise on a bipartisan basis. Clifford, a "veteran of Democratic politics, [who] is one of the capital's most widely sought attorneys, and a trusted private adviser to the President," represented something of a departure.[93] Clifford's appointment was the first time someone known largely for being a "Washington fixer" had ever been appointed to the board; moreover, he was appointed with the additional understanding that he would be Killian's successor as chairman in just a few months.

Besides not appreciating, along with his colleagues, McCone's alleged effort to cut off PFIAB's direct access to the president, Clifford also took exception to McCone's outspokenness as director of Central Intelligence. McCone "did not submerge his strong personal opinions inside official assessments in the manner of most senior intelligence officers," Clifford would later write, not knowing or impervious to the fact that President Kennedy had expressly asked McCone to express his policy views.[94] And the fact that the press, after the missile crisis, was hailing McCone for being the only senior official to predict that the Soviets would implant missiles in Cuba displeased Clifford greatly.[95] The friction between the suave lawyer and blunt, engineer-turned-tycoon would reach, in Clifford's words, a "crescendo" during the missile crisis post-mortem.[96]

Although the record of PFIAB's deliberations is spotty, there are some extant and revealing primary documents, and the one panel member who was almost certainly the most influential in shaping the post-mortem—Clark Clifford—fortunately wrote about the episode in some detail. When PFIAB began contemplating a review of the intelligence aspects of the crisis, "we were faced with a dilemma," according to Clifford. "We did not wish to criticize the President, who had handled the crisis brilliantly once the Soviet missiles had been positively identified by American intelligence," wrote Clifford, "but we felt the length of time it had taken to discover the missiles was dangerously and inexcusably long. We were particularly disturbed that there had been no overflights of Cuba between August 29 and October 14 despite public charges that offensive missiles were being installed."[97] Thus, if Clifford's memoir is taken at face value, it seems that he and the other PFIAB members correctly identified the key operational deficit early on, and instantly recognized its political sensitivity.[98]

PFIAB's own deliberations began in earnest in early December, when McCone appeared to discuss the mechanics of the USIB post-mortem and answer the panel's questions in person. In tow were Lieutenant General Carroll, director of the DIA; Lyman Kirkpatrick, executive director of the CIA (and the DCI's liaison with PFIAB); and Richard Helms, the Agency's deputy director of Plans (DD/P). McCone had voluntarily provided PFIAB with a copy of the Lehman report, and had also mentioned the existence of the IG report.[99] After briefing the panel on the scope and progress of the USIB report, McCone said he thought it would be a good idea for PFIAB to have its own special briefing on clandestine operations in Cuba in order to see precisely how they had contributed to the intelligence mosaic leading to the missiles' discovery. The panel then heard from Richard Helms about the human intelligence that had been provided, particularly by agents recruited under MONGOOSE, one of whom had been instrumental in pinpointing the trapezoid-shaped location where the first SSMs were discovered.[100]

After Helms's presentation ended, and in response to questions, McCone mounted a stout defense of the intelligence community's performance, minimizing the estimative, analytical, and operational deficits. It was akin to an "all's well that ends well" perspective. At one juncture, former diplomat Robert Murphy asked if "any handicaps had been placed on the collection of intelligence about Cuba."[101] Here, if the DCI wanted it, was an opening to apportion responsibility for the degradation of U-2 surveillance in September. But McCone, acting as an administration loyalist, eschewed the opportunity to criticize policy makers for putting blinders on the CIA. "No," answered McCone, before he briefly recounted the establishment of a CIA agent network recruited under MONGOOSE.[102]

At this juncture the questioning became more pointed. Clark Clifford brought up the issue of McCone's personal estimate regarding Soviet offensive missiles, first enunciated in August, and also asked about distribution of the so-called honeymoon cables.[103] "Then these telegrams had not gone anywhere outside

CIA?" asked PFIAB member Gordon Gray. "No," replied McCone, explaining that "it would have been wrong to go over the head" of Marshall Carter, the acting DCI, by disseminating these cables to the principal members of the USIB.[104] Frank Pace, another PFIAB member, then asked point-blank the critical question: How much earlier than mid-October might the U-2 have discovered offensive missiles? McCone responded that uncovering the missiles was conceivable from about September 20 onwards but claimed that nothing clinching the case was likely until mid-October. Besides demonstrating his loyalty in private to the administration's public position, the DCI was foreshadowing the negotiated finding of the USIB post-mortem.

Throughout the grilling, McCone replied in a very measured way and recited the facts mostly without characterizing them. He referred briefly to the "timidity" and "attitude of caution" that existed in September but the relaxed attitude about the consequences that existed now—a posture at considerable odds with his actual position in late September/early October.[105] "There was nothing convincing" until the intelligence community conducted the mid-October aerial surveillance, McCone asserted.[106] But that perspective was not very persuasive to the PFIAB members. They probably regarded it as evidence of McCone's belief that any post-mortem conducted by PFIAB (if not the board itself) was more of a hindrance than a help. McCone's appearance primarily served to harden PFIAB's inclination to take a close look at the USIB's post-mortem.

Even before the final draft arrived, PFIAB began drawing up its own lessons learned, with Clark Clifford acting as the prosecuting attorney. Clifford argued, with apparent persuasiveness, that not only had the CIA been remiss in its photo coverage, but McCone had been derelict for failing to push the intelligence community into "making a more intensive effort to corroborate his [own] beliefs" about the likelihood of a Soviet deployment.[107] Clifford intimated, moreover, that McCone had put his personal life before his official duties by being absent from Washington during a crucial period. "From France [McCone] sent strongly worded personal messages—the so-called honeymoon cables . . . but he still did nothing to speed up the pace of air reconnaissance," as Clifford later put it.[108] This was a tendentious rendering of the situation that prevailed in Washington in late August. At that time McCone's hunch was based primarily on intuition and was otherwise unsupported except by refugee reports that had proven to be uniformly mistaken.[109]

Once the PFIAB received the USIB report on December 26, weeks later than originally promised, the board met immediately to discuss the coordinated findings. McCone personally presented the USIB post-mortem, but after the DCI left, Clifford declared himself profoundly unimpressed. As he later wrote, Clifford bluntly labeled the report a "snow job" because of the way it depicted the photo gap, and criticized the excessive "delicacy" with which the issue of U-2 overflights had been addressed.[110] "Everyone was pointing the finger at someone else," Clifford wrote, although presumably, sorting out who did what, when, and why, was precisely the point of any post-mortem.[111] To a degree, of course, the

urbane Washington lawyer was right. The USIB report was a "snow job," attributable to the fact that it was a coordinated history drafted by the same offices that had collected and evaluated the intelligence. Still, the direction in which the post-mortem was bent insulated the Kennedy administration from criticism, at least as much, if not more than, it benefited the intelligence community.

Clifford then posed a direct question to his colleagues: If a similar situation were to be encountered again, would anyone on PFIAB argue that the president had been well served by the intelligence community? There was silence—until Clifford answered his own question. The successful outcome of the missile crisis should not "lull us into a false sense of comfort," he argued.[112] And then Clifford openly inserted a political consideration into PFIAB's deliberations. The Republican National Committee had leveled a "preposterous" allegation against President Kennedy, namely, that he had deliberately withheld and/or manipulated information about the missiles in order to gain a political advantage.[113] The facts proved otherwise, said Clifford, and had to be brought out in PFIAB's own report because the intelligence community was obviously unwilling to face up to its own shortcomings. "The delays had been caused by decisions made *within the intelligence community* for internal reasons," declared Clifford (emphasis added).[114] The outstanding deficit was "the state of mind within the intelligence community . . . which rejected the possibility of offensive missiles in Cuba." And he was concerned that the president "would be hurt by the CIA's efforts to protect itself."[115] In sum, Clifford was aiming to shift the entire onus for the photo gap onto the CIA, if not a Republican DCI.

Despite the sharp questions from PFIAB members, McCone had left the meeting on December 28 apparently unaware of the depth of their dissatisfaction with the USIB report. When he met with the president on January 7, the subject of the PFIAB study came up, an interim version of which had been submitted to the White House on December 28.[116] McCone thought it was good insofar as it went, though it was mostly prescriptive. PFIAB's findings about the community's pre-October performance had yet to be incorporated. McCone nonetheless used the occasion to express his own unvarnished beliefs to Kennedy directly for perhaps the first time. The IC had done a good job but "could have done better," observed McCone.[117] The principal errors were, in order, the photo gap; the estimative deficit; and last, the failure to analyze correctly some indicators that might, in retrospect, have challenged the estimate. With respect to the photo gap, McCone was careful to spread responsibility around, noting that it was due to "timidity throughout the government."[118] In response, the president said little but did express sympathy for the estimators' plight. In effect, Kennedy adopted what would be Sherman Kent's formulation: that the Soviets' estimate (if there in fact was one) of the U.S. reaction to the missile deployment was the most flawed estimate of them all.[119]

PFIAB, meanwhile, pressed ahead with its study. According to Clifford's memoir, this involved gaining access to material and information that went beyond the post-mortems and briefings McCone had made available. When

McCone allegedly refused to provide more materials, Clifford declared the DCI's obstructionism intolerable. "If McCone was going to set himself up as a censor of what the PFIAB could and could not see," Clifford later wrote, "then [PFIAB's] functions and rationale would be destroyed."[120] Clifford threatened to resign, and when President Kennedy heard about the dispute he reportedly instructed McCone to be forthcoming. Even so, from Clifford's perspective "a breach had been opened with McCone" that would remain until the end of his tenure.[121]

On February 4, 1963, PFIAB submitted its final report to the White House, and little more than a month later the findings were presented directly to President Kennedy during a seventy-nine-minute meeting on March 9.[122] The PFIAB post-mortem read more like a lawyer's brief than a disinterested analysis, something the president could use to rebut the Republicans' uphill efforts to attack his handling of the crisis. PFIAB concluded that the intelligence community achieved a very high level of performance between October 14 and 22, 1962, but the same could not be said of the pre-October 14 period. The "Soviet move came dangerously close to success," noted the report, primarily because there was not, within the intelligence community, a "focused sense of urgency or alarm which might well have stimulated a greater effort."[123] Specifically, PFIAB found the community's effort deficient in two areas: the acquisition of intelligence via human assets in Cuba and the failure to make "full use" of aerial surveillance, particularly during September and October.[124] Responsibility for the photo gap was put squarely in the lap of the intelligence community, which failed "as a whole to propose to the Special Group U-2 reconnaissance missions on a scale commensurate with the nature and intensity of the Soviet activity in Cuba . . . . [especially] in view of the inadequacy of clandestine agent resources."[125]

PFIAB's analysis, markedly influenced by Clifford, was almost transparent in its effort to absolve policy makers from any responsibility for the photo gap. The longest paragraph in PFIAB's ten-page post-mortem pertained to the September 10 meeting. Owing to the paucity of records, the board claimed it was "impossible to determine whether or not there was a restriction" that prevented intrusive overflights of Cuba, although PFIAB did allow that the CIA was clearly under the "impression" that such an injunction was imposed.[126] But rather than apportion the consequences of the photo gap in a fair manner, PFIAB only found fault with the intelligence community. In what was becoming a familiar litany, the president "granted authorization for all U-2 flights which were recommended to him by . . . the Special Group [Augmented]."[127] The SGA "was not made fully aware of the delaying effects on the acquisition of aerial intelligence" that stemmed from the September 10 decision, and the SGA "should have been informed of the factors operating to delay the four-flight coverage, and given an opportunity to reconsider the advisability of a mission over the critical target areas urgently requiring surveillance."[128] Such a judgment betrayed definite bias and one-sided critique. As everyone involved in the U-2 program knew, one of the fundamental ways the Special Group and the president imposed managerial

discipline on the overflight regime was to insist upon completion of approved flights before they would entertain new requests.[129]

McCone was not one to let PFIAB's post-mortem go unchallenged; in fact, he was seething about the criticism, which he apparently considered akin to Monday-morning quarterbacking.[130] In a February 28 memorandum to President Kennedy he defended the performance of the intelligence community, especially with regard to the photo gap. Somewhat ironically, doing so put McCone in the position of at least partly defending the timid overflight policy he had so vigorously lobbied against the previous fall. The "reluctance or timidity" to direct U-2 flights over Cuba was understandable in context, McCone now contended, given the severe international criticism of such flights dating back to the Francis Gary Powers incident in May 1960.[131] Admittedly, the intelligence community had failed to communicate adequately the consequences that flowed from the September 10 decision and the urgency of resuming more intrusive overflights, noted McCone.[132] Anyone reaching such a conclusion, however, "must first carefully weigh the serious considerations that enter into a decision to overfly denied territory," the DCI observed.[133] McCone reminded the president that he was not an intelligence careerist determined to defend the community's performance against any and all criticism, and that his own estimate had differed from that of all the experts. Still, after examining the community's performance with a "critical eye," he believed the coordinated USIB post-mortem "reflect[ed] a more reasonable judgment of the performance of the intelligence community in the six months' period prior to the October crisis" than PFIAB's findings.[134] The USIB post-mortem was certainly more congruent with the administration's public position than the PFIAB report, though McCone left this unsaid.

The dispute over whose post-mortem was more accurate did not end there. PFIAB responded to McCone's rejoinder, and the board's deliberations continued into March 1963, according to Clifford's memoir. In what was apparently the last meeting on the subject, former Ambassador Robert Murphy, speaking for the panel, told McCone that PFIAB "had reached the conclusion that there had been a significant intelligence failure," and that it was their duty to report as much to the president. McCone, according to Clifford, responded angrily, and stated that Murphy was "misstating the facts."[135]

PFIAB's "important" post-mortem cast a jaundiced eye on the intelligence community's performance.[136] That was fair enough, especially in light of the coordinated USIB report, which tended to explain (and implicitly excuse) all the deficits.[137] Yet it is impossible to separate out the harshness of PFIAB's findings from the fact that many board members were "averse" to John McCone, as Robert Kennedy would put it in 1964.[138] McCone "had made a lot of enemies," several of whom were on PFIAB, and this was an opportunity to strike back—or, at least, dim the luster of the Agency's achievement under McCone's stewardship.[139] Consequently, in its eagerness to tarnish the CIA's performance, and cut down McCone's newly won reputation for prescience, PFIAB erred in the other direction, taking the deficits out of the context in which they had occurred, as if the

intelligence community operated in a vacuum, immune from the pressures or concerns of policy makers.[140] Such a perspective diminished the accuracy and usefulness of PFIAB's post-mortem, because when all was said and done, discovery of the missiles before they became operational was vital to a peaceful resolution of the crisis, and thus, represented the CIA's "finest hour" of the Cold War—according to almost everyone but PFIAB. In place of an objective and dispassionate report, the president's board produced a handy tool for rebutting Republican charges about the administration's performance, which certainly served what was Clifford's primary interest.[141]

About a month after PFIAB finished work on its post-mortem, Clifford was elevated, as planned, to chairmanship of the board.[142] The august *New York Times* thought so ill of Clifford's ascension in intelligence matters that it ran an editorial criticizing the appointment.[143] Clifford "has a brilliant mind," observed the *Times,* "but, as a long-time trouble-shooter for the Democratic party, he is inextricably associated with partisan politics. The selection is at best unfortunate. It is bound to give the impression that our intelligence activities will now be monitored—not by a chairman who is an expert in the field—but by one who is essentially a politician."[144] It is not known whether the *Times*' editorial writer knew about the raging internal dispute over PFIAB's critical post-mortem. If not, he was as prescient about Clifford's influence on PFIAB as McCone had been about the emplacement of Soviet missiles.[145]

CONCLUSION

Weeks after the missile crisis subsided, DD/I Ray Cline asked both McGeorge Bundy and Robert Kennedy how much the CIA's photo surveillance of October 14 was worth to the nation. Both responded that it fully justified all the CIA had cost the country since its inception in 1947.[146] None of the four classified post-mortems made this precise point, although they were certainly unanimous in believing that the CIA's discovery of the first missiles in mid-October was critical.

A close analysis of each post-mortem shows at least three of the four differed substantially on another crucial point: why the missiles' discovery was delayed, and who or what was responsible for that tardiness. The Lehman and IG reports, insofar as they are known, were in close agreement over the plain facts and their meaning. But as responsibility for an ex post facto analysis moved outside the confines of the CIA, both facts and their meaning became increasingly contested. The first result was a post-mortem that deliberately muddled the narrative of what had happened and why (the USIB account) and then a PFIAB report to the president that turned the story nearly upside down. Put another way, the analyses careened from one that simply recounted the somewhat messy, nontextbook manner in which the missiles had actually been discovered, to one that asserted the nation had in fact experienced a nearly catastrophic intelligence failure, owing solely to the CIA's dereliction of its responsibilities. The four post-mortems bring

to mind Akira Kurosawa's film masterpiece *Rashômon.* When each one is examined closely, it cannot be separated from the person(s) who wrote it and the external or extraneous circumstances involved in its production.

What makes this finding all the more sobering is that this intense struggle over assessments, if not history itself, occurred completely behind the scenes, and over a crisis that was widely considered an unmitigated triumph for the incumbent administration. If there was so much disagreement and difficult bargaining over an intelligence success, it must be incomparably more difficult to reconcile competing interests when an intelligence failure is the subject of the inquiry. And conducting a post-mortem outside the intelligence community seems only to compound the problems inherent in producing objective history, as evinced by the contemporaneous findings of the Senate Preparedness Subcommittee, the only congressional panel to mount an investigation into intelligence aspects of the missile crisis. The subcommittee's 1963 report "examined this question [of an alleged photo gap] as thoroughly as possible and . . . found the allegations with respect to it to be *unfounded*" (emphasis added).[147]

For all their problems, post-mortem exercises would seem clearly desirable under controlled conditions. In fact, the argument could be made that one of the chief failings of the intelligence community as it existed until 2004 was that post-mortems occurred too irregularly, and on an ad hoc basis when they occurred at all. There was only one sustained effort to institutionalize a rigorous and systematic post-mortem program, and that occurred in the 1970s. For roughly two years, from late 1973 to late 1975, the DCI, together with the USIB, mounted a program that resulted in the production of seven post-mortems on a variety of topics. But the effort was soon abandoned after the unfortunate confluence of internal and external factors. Inside the community many officers opposed post-mortems on the grounds that "candid critical reviews" offered "at best, an unbalanced look at the condition of the profession and, at worst, [were] an unnecessary exercise in self-flagellation."[148] Externally, the House Select Committee on Intelligence (a.k.a. the Pike Committee) all but sounded the death knell for the program when it attempted to wield the post-mortems against the very community that had produced them.

In the absence of demanding standards and objective procedures for conducting post-mortems, the lesson from 1962–63 would seem to be that all such inquests should be viewed critically, and with the utmost caution. They can easily be as flawed as the intelligence product and process they purport to judge, if not more so. After all, not knowing the future at least imposes a certain degree of honesty. With the benefit of hindsight, everyone knows what side to be on.

NOTES

This article is adapted from one originally prepared for the *International Journal of Intelligence and CounterIntelligence*, and appears with gracious agreement of that journal's editor.

1. Chris Strohm, "Intelligence Chiefs Cite Advancements, Challenges," *Government Executive*, March 9, 2004.

2. Some post-mortems have been subject to immediate discount, most often when they were competing with a contemporaneous congressional probe. See, for example, public reaction to the *Report to the President by the Commission on CIA Activities Within the United States* (Washington, DC: U.S. Government Printing Office, 1975), a.k.a. the Rockefeller Commission, or the *Report of the President's Special Review Board* (Washington, DC: U.S. Government Printing Office, 1987), a.k.a. the Tower Commission.

3. For a recent work that explores the nature of several blue-ribbon panels, see Kenneth Kitts, *Presidential Commissions & National Security: The Politics of Damage Control* (Boulder, CO: Lynne Rienner, 2006).

4. A fifth, semi-public post-mortem was conducted by the Senate Armed Services' Subcommittee on Preparedness, chaired by Senator John Stennis (D-MS). This interim report was published in 1963, but the hearings were conducted in secret. It is not included in this chapter, though it well might be, because it involved two variables not present in the other inquiries: political partisanship over a post-mortem intended for public consumption, and limited access to the necessary information. The subcommittee relied primarily on testimony from administration officials taken in executive session. U.S. Senate, Committee on Armed Services, Preparedness Investigating Subcommittee, "Investigation of the Preparedness Program: Interim Report on the Cuban Military Buildup" (Washington, DC: U.S. Government Printing Office, 1963).

5. In chronological order, the post-mortems were: Memorandum for the Director of Central Intelligence, "CIA Handling of the Soviet Build-up in Cuba, 1 July–16 October 1962," November 14, 1962 (hereafter Lehman Report); Memorandum for DCI McCone from J. S. Earman, Inspector General, "Handling of Raw Intelligence Information During the Cuban Arms Buildup," November 20, 1962 (hereafter IG Report); "Report to the President's Foreign Intelligence Advisory Board on Intelligence Community Activities Relating to the Cuban Arms Build-up (April 14 through October 14, 1962) by the Director of Central Intelligence," December 26, 1963 (hereafter USIB Report); and "Report of the President's Foreign Intelligence Advisory Board on the Soviet Military Build-up in Cuba," February 4, 1963 (hereafter PFIAB Report). In 1992 four pages of the Lehman Report, and the entire PFIAB Report, were excerpted in Mary McAuliffe, ed., *CIA Documents on the Cuban Missile Crisis* (Washington, DC: Central Intelligence Agency, October 1992), pp. 99–102, 361–71. A sanitized version of the USIB Report first became available in 1998 under provisions of the John F. Kennedy Assassination Records Collection Act; in 2004 more complete versions of the USIB and Lehman Reports were released via the CIA Records Electronic Research Tool (CREST) at the National Archives in College Park, Maryland (hereafter NARA). The Earman post-mortem is cited in an official history of the U-2 (Gregory Pedlow and Donald Welzenbach, *The CIA and the U-2 Program,* Washington, DC: Central Intelligence Agency, 1998), p. 206. At this writing, however, this document has not been released via CREST, and in response to a 2003 Freedom of Information Act request, the CIA wrote that it was unable to locate the report. Letter, CIA Information and Privacy Coordinator to the author, December 22, 2005.

6. The four post-mortems were essentially unanimous in their praise of the intelligence community's work after the discovery of Soviet missiles on October 15, 1962.

7. As the *New Yorker*'s Washington correspondent observed, "the handling of the October crisis was, of course, superb (an easy *ex-post-facto* judgment, based wholly

upon success)." Richard Rovere, "Letter from Washington," *New Yorker,* March 2, 1963.

8. "The Cuban Missile Crisis, 1962," in *Deterrence in American Foreign Policy: Theory and Practice,* eds. Alexander George and Richard Smoke (New York: Columbia University Press, 1974), p. 473. Decades later, another scholar would label the pre-October 14 intelligence product "deficient due to *operational,* as much as *analytical,* reasons" (emphasis in the original). Gil Merom, "The 1962 Cuban Intelligence Estimate: A Methodological Perspective," *Intelligence and National Security* (hereafter *I&NS*) 14 (Autumn 1999), p. 52.

9. September 17–18 was subsequently fixed as the earliest date after which SSMs might have been detected, had there been constant and intrusive aerial surveillance. CIA/Office of Research and Reports, "Cuba 1962: Khrushchev's Miscalculated Risk," February 13, 1964, National Security File, Country File: Cuba, Box 35, Lyndon B. Johnson Library (hereafter LBJL), pp. 2–3.

10. As one respected scholar of the intelligence process later wrote, it really should not have mattered "what intelligence 'thought' " about the likelihood of missiles being deployed in Cuba. "But it did matter, imperatively, that intelligence collect the data which would permit a firm judgment whether or not the missiles were there." Cynthia Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Lanham, MD: University Press of America, 2004), p. 140.

11. Hanson Baldwin, "An Intelligence Gap: Experts Ask If Reports on Cuba Were Poor or Adapted to Policy," *New York Times,* October 31, 1962. If the estimates had been tailored, the article suggested that an alleged overcentralization of intelligence was likely the cause, because it might have created an IC "unduly influenced by the knowledge of what current policy was."

12. "The Military Build-up in Cuba," SNIE 85-3-62, in *CIA Documents,* ed. McAuliffe, pp. 91–93.

13. Max Holland, "Politics and Intelligence: The 'Photo Gap' That Delayed Discovery of Missiles in Cuba," *Studies in Intelligence* (hereafter *SII*) 49 (2005), pp. 15–30.

14. Max Frankel, *High Noon in the Cold War: Kennedy, Khrushchev, and the Cuban Missile Crisis* (New York: Ballantine, 2004), p. 27. In his history/memoir, McGeorge Bundy hinted at the significance of the photo gap, which otherwise received short shrift in his book. "The photographs of October 14 were taken in good time, but they had been delayed, first by our own caution in overflying Cuba. . . . If our primary interest here were in the intelligence process, these matters would deserve further attention." McGeorge Bundy, *Danger and Survival: Choices About the Bomb in the First Fifty Years* (New York: Random House, 1988), p. 687. That the crucial October 14 overflight induced great anxiety in the administration, and only received approval by a slim margin, was evinced by a remark made during a conversation on October 12 between DDCI Marshall Carter and U.S.A.F. General William McKee, vice chief of staff under General Curtis LeMay. "This is the most overcontrolled operation I've ever been in," McKee observed to Carter. Second conversation between General Carter and General McKee, October 12, 1962, released to the author under the Freedom of Information Act (hereafter FOIA), December 2005.

15. Besides being a primary topic of the official post-mortems, the misestimates and analytical shortcomings have been extensively written about in the intelligence-related literature about the crisis. See Sherman Kent, "A Crucial Estimate Relived," *SII,* Spring 1964; George and Smoke, *Deterrence,* pp. 477–81, 488–91; Raymond Garthoff,

"US Intelligence in the Cuban Missile Crisis," *I&NS* 13 (Autumn 1998), pp. 20–26; and Merom, "1962 Cuban Intelligence Estimate," pp. 48–80.

16. In his posthumously published memoir of the crisis, Robert Kennedy would admit, "We had been deceived by Khrushchev, but we had also fooled ourselves." Yet Kennedy was far from specific about how close his brother's administration had come to being surprised by the deployment of operational missiles. Robert Kennedy, *Thirteen Days: A Memoir of the Cuban Missile Crisis* (New York: W.W. Norton, 1969), pp. 27–28, and Holland, "Photo Gap," pp. 27–28. Not all students of the crisis agree that the photo gap was an exceptionally sensitive issue. See James Blight and David Welch, "What Can Intelligence Tell Us About the Cuban Missile Crisis, and What Can the Cuban Missile Crisis Tell Us About Intelligence?" *I&NS* 13 (Autumn 1998), p. 6. According to these scholars, it was "for the most part a red herring—less interesting to students of intelligence than to followers of sordid Camelot sub-plots."

17. John Helgerson, *CIA Briefings of Presidential Candidates, 1952–1992* (Washington, DC: Center for the Study of Intelligence, 1996), p. 69.

18. Ibid., p. 66.

19. Richard Kovar, "Mr. Current Intelligence: An Interview With Richard Lehman," *SII* 9 (Summer 2000), p. 57; Helgerson, *CIA Briefings,* p. 67.

20. "For current intelligence people, [the President's engagement with the PICL] was heaven on earth!" Russell Jack Smith, *The Unknown CIA: My Three Decades With the Agency* (Washington, DC: Pergamon-Brassey's, 1989), p. 149.

21. Strictly speaking Marshall Carter, Deputy Director of Central Intelligence (DDCI), was the first high official to ask for a post-mortem; Carter probably anticipated that criticism for the photo gap would be directed at him because he had been acting DCI when the coverage was degraded. James Reber, Chairman of the Committee on Overhead Reconnaissance (COMOR), submitted a memorandum to Carter on October 24, 1962, in response to the DDCI's request. Reber concluded, in the midst of the crisis, that nothing had indicated "that any other approach would have served us better." Of course, Reber had some reason to be defensive also, as the White House might claim that the COMOR, charged with developing overflight requirements, failed to keep the president fully apprised of the dysfunctionality of the surveillance regime after September 10. Memorandum for DDCI, "Historical Analysis of U-2 Overflights of Cuba," October 24, 1962, released under FOIA, December 2005.

22. Kovar, "Mr. Current Intelligence," p. 57.

23. On the copy of the Lehman Report released under CREST, there is a handwritten notation on the title page: "Save for the Pearl Harbor hearings—if some, or any." Lehman Report, CREST, NARA.

24. Walter Elder, "John A. McCone: The Sixth Director of Central Intelligence," 1987, Box 1, CIA Miscellaneous Files, John F. Kennedy Assassination Records Collection, NARA, p. 38.

25. Kovar, "Mr. Current Intelligence," p. 57. The Lehman Report via the CREST system does not include any annexes.

26. Smith, *Unknown CIA,* p. 149.

27. Lehman Report, p. 12.

28. A routine U-2 overflight on August 29 had uncovered the first evidence of SA-2s being emplaced on Cuba, the same SAM that had downed Francis Gary Powers's aircraft in May 1960. Completely coincidentally, the growing threat to U-2 overflights of the

island was underscored by two distant incidents in early September. On August 30 an air force U-2 had violated Soviet airspace for nine minutes during an air-sampling mission, and on September 9, a U-2 manned by a Taiwan-based pilot was lost over mainland China. Pedlow and Welzenbach, *The CIA and the U-2 Program,* p. 201.

29. Holland, "Photo Gap," pp. 19–21.

30. Interview with Richard Lehman, April 14, 2003.

31. Portions of the Lehman Report are still closed, and the annexes are apparently unavailable, so it is not possible to state the precise details Lehman left out. One example of an omitted detail might be the fact that at 3 pm on September 10, McGeorge Bundy had rescinded approval of the one remaining September overflight, presumably to demonstrate the administration's seriousness about avoiding a U-2 incident over Cuba. DD/R Memo for the Record, "Cuban Overflights," September 10, 1962, CREST, NARA.

32. Scoville maintained that the most important objective of the October 14 U-2 mission was coverage of the so-called San Cristóbal trapezoid, whereas Lehman suggested overflying an advanced SAM site in western Cuba had actually been a higher priority. For his part, McCone insisted that it was "erroneous to give the impression [that] this flight went where it went because we suspected [offensive missiles] were there. This was simply not the case." These divergent perspectives reflect the struggle that occurred in early October over resuming more intrusive U-2 overflights. Scoville was apparently more familiar with how the U-2 requirements were specifically developed on the basis of human intelligence, while the DCI was closer to the rationales behind the necessary approvals at the highest levels, for example, within the Special Group Augmented and inside the Oval Office. See Memo, DDR to DCI, "Comments on Lehman Paper," November 7, 1962, and "Notes for Mr. Earman," December 17, 1962, both in CREST, NARA; and Holland, "Photo Gap," pp. 25–26.

33. Lehman Report, p. 29.

34. During the Kennedy administration the Special Group, an interagency subcommittee of the National Security Council, oversaw all covert activity, including U-2 surveillance; the Special Group Augmented dealt solely with Cuba.

35. "John S. Earman Jr., 60," *Washington Post,* April 11, 1974.

36. Wrote Earman, "On 21 November you [McCone] asked me to consider two additional conclusions for my report." Memorandum for DCI, "Inspector General's Report on Handling of Intelligence Information During the Cuban Arms Build-Up (Revised), dated 20 November 1962," November 26, 1962, CREST, NARA.

37. Ibid.

38. Ibid.

39. Ibid.

40. As with the Lehman Report, Scoville reviewed the IG post-mortem. "From all the information available to the DD/R, it is believed that the report of the Inspector General is factually accurate," Scoville wrote. Memorandum for Deputy Director of Central Intelligence, "Handling of Intelligence Information During the Cuban Arms Build-up," December 15, 1962, CREST, NARA.

41. Memorandum for Director of Central Intelligence, "Department of State's Objections to the Report on the Cuban Arms Build-up," March 12, 1963, CREST, NARA.

42. Simultaneously, the president asked McCone personally for the same type of report. Memorandum of the Record, "Meeting with PFIAB, 7 December 1962," December 10, 1962, CREST, NARA.

43. PFIAB was originally called the President's Board of Consultants on Foreign Intelligence Activities, and created by Eisenhower based upon a recommendation of the second Hoover Commission. *The President's Foreign Intelligence Advisory Board* (Washington, DC: Hale Foundation, 1981), p. 1.

44. Memorandum for Director of Central Intelligence, "Department of State's Objections to the Report on the Cuban Arms Build-up," March 12, 1963, CREST, NARA.

45. At the time, one of the ways the DCI coordinated the intelligence effort was through the machinery of the USIB, which consisted of representatives from all the intelligence agencies, for example, the deputy director of CIA (General Marshall Carter), who represented the CIA; the directors of INR (Roger Hilsman), DIA (Lieutenant General Joseph Carroll), NSA (Lieutenant General Gordon Blake); the intelligence director for the Joint Chiefs of Staff (Major General Richard Collins); the assistant director (Alan Belmont) of the Federal Bureau of Investigation (FBI); and the assistant general manager for administration (Harry Traynor) of the Atomic Energy Commission. The heads of Army, Navy, and Air Force intelligence (respectively, Major General Alva Fitch, Rear Admiral Vernon Lowrance, Major General Robert Breitweiser) also attended USIB meetings as observers. The USIB met weekly, sometimes more frequently, and among other things rendered advice on National Intelligence Objectives (NIOs) and the production of National Intelligence Estimates (NIEs), two of the DCI's most important responsibilities. Statement for the Record, Document 21b, Central Intelligence Agency, Vol. II, Box 9, National Security File, Presidential Papers, LBJL; Memorandum of the Record, "Meeting With PFIAB, 7 December 1962," 10 December 1962, CREST, NARA.

46. Memorandum for the Record, "DCI Meeting With PFIAB," 7 December 1962, CREST, NARA.

47. The other working group members (as chosen by their respective agencies) were William McAfee, director of the Coordination Staff of the State Department's INR; Samuel Halpern, executive officer of the CIA's Task Force W on Cuba, representing the DD/P; a representative from the DIA's Office of Estimates; the chief of the DIA's Current Intelligence Indications Center; the deputy chief of the NSA's Policy Division; and the CIA's deputy assistant director for Central Reference, representing the DD/I.

48. DD/R Memo, "Cuban Missile Crisis," November 13, 1962, CREST, NARA.

49. Memorandum for Deputy Director (Research), "Interagency Review of Intelligence Activities Relating to the Cuba Situation," November 26, 1962, CREST, NARA.

50. After the meeting, Reber had reportedly observed, "When men of such rank involve themselves in planning mission tracks, good intelligence officers just listen." Dino Brugioni, *Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis* (New York: Random House, 1990), p. 138.

51. Memorandum for Deputy Director (Research), "Interagency Review of Intelligence Activities Relating to the Cuba Situation," November 26, 1962, CREST, NARA.

52. Recounting the facts for the questionnaire was fraught with problems. The DIA's answers, for example, placed that agency at the forefront of the decision to overfly the San Cristóbal trapezoid, although the truth was a bit more complicated. DIA, "Use of Intelligence Product," undated, CREST, NARA, and Holland, "Photo Gap," p. 25.

53. Memorandum for Deputy Director (Research), "Interagency Review of Intelligence Activities Relating to the Cuba Situation," November 26, 1962, CREST, NARA.

54. The detailed memorandum about the pivotal September 10 meeting printed in the relevant *Foreign Relations* volume was prepared well after the fact, that is, on

February 28, 1963. Acting DCI Marshall Carter wrote only a one-paragraph summary about the unusual meeting, and the only other contemporaneous record was a September 11 memo by Thomas Parrott, the assistant to General Maxwell Taylor, who was then the president's military representative. See "Memorandum Prepared in the Central Intelligence Agency for the Executive Director," dated September 10, 1962 (but prepared February 28, 1963), U.S. Department of State, *Foreign Relations of the United States (FRUS), 1961–1963,* Volume X: *Cuba 1961–1962* (Washington, DC: U.S. Government Printing Office, 1997), pp. 1054–55, and Document 296, "Acting," September 10, 1962, *FRUS,* Vol. X, Microfiche Supplement. The Parrott memorandum was cited in the USIB Report, pp. 69–70. See also Memorandum for the Record, "Telephone Conversation With Mr. Tom Parrott on 10 September Concerning IDEALIST Operations Over Cuba," September 10, 1962, CREST, NARA, and Memorandum for the Director, "White House Meeting on 10 September 1962 on Cuban Overflights," March 1, 1963, in McAuliffe, ed., *CIA Documents,* pp. 61–62.

55. Once, during a USIB meeting on September 19, acting DCI Carter remonstrated about the attenuation of U-2 overflights. "We cannot put a stop to collection," Carter fumed. "Otherwise, the president would never know when the point of decision was reached." McAuliffe, ed., *CIA Documents,* p. 42. CIA officials' willingness (apart from McCone) to accede to policy makers on the overflight regime probably was a consequence of the general disfavor in which the Agency was held by the administration following the Bay of Pigs.

56. Roger Hilsman Oral History, August 14, 1970, John F. Kennedy Library (hereafter JFKL), p. 4.

57. Ibid., p. 15.

58. Referring to the highly secret PICL prepared daily by Richard Lehman, Hilsman observed, "In McCone's day they [CIA] didn't play honest with me in that they did get out sort of a private thing for the President, which they tried like hell to keep anybody from seeing who wasn't too important." Hilsman tried to develop a rival publication, called the "Intelligence Note," which was an INR document of 300 hundred words or less that he would disseminate within six hours of an overseas event. "He who gets the first interpretation out commands the field," noted Hilsman. The INR director was also rankled by the fact that he had no authority or say over covert activities presented to the 5412 Group; the Under Secretary of State represented the State Department in the Special Group. Finally, when McCone was appointed DCI, Hilsman was furious with Rusk for not consulting him beforehand, and the INR director was one of the administration officials who energetically opposed the nomination of an "alley fighter" who was "a very rich . . . very militant, anti-communist Republican." Ibid., pp. 8–9, 13, 15. Because of opposition from liberal New Frontiersmen like Hilsman, McCone received more negative votes in the Senate than any DCI nominee had ever received.

59. Interview with Harold Ford, July 2, 2005. In a manner not appreciated by DD/R Scoville, for example, Hilsman had tried to insert himself in the decision-making process that led to the September 10 decision regarding U-2 overflights. Memorandum for the Record, "Telephone Conversation With Mr. Tom Parrott on 10 September Concerning IDEALIST Operations Over Cuba," September 10, 1962, CREST, NARA.

60. U.S. Department of State, *FRUS, 1961–1963,* Volume XI: *Cuban Missile Crisis and Aftermath* (Washington, DC: U.S. Government Printing Office, 1996), Document 323, "Conversation Between General Carter and Roger Hilsman," October 16, 1962, *FRUS,* Vol. XI, Microfiche Supplement.

61. Ibid.

62. Hilsman Oral History, pp. 6, 16, JFKL. McCone's prescience, ironically, did not win him admission into the president's inner circle; in fact, his stock with the Kennedys declined. Holland, "Photo Gap," pp. 29–30.

63. Memorandum for Director of Central Intelligence, "Additional Inspector General Conclusions on Cuban Arms Build-up," November 28, 1962, CREST, NARA.

64. "Notes for Mr. Earman," December 17, 1963, CREST, NARA.

65. McCone added that the CIA "had been remiss in proposing something less than complete coverage," having been overly influenced by policy makers intent on avoiding a U-2 incident. Ibid.

66. On December 26 Hilsman had second thoughts about the language of the sixth draft after it was agreed upon by the USIB working group and steering committee. According to a memo from Marshall Carter to McCone, Hilsman called Carter "with about 25 proposed changes to the final draft report. Some have great merit and others are nitpicks. I explained to him . . . that we could keep rewording the thing for months and not satisfy everyone, that we must presume that the Killian Board is friendly . . . and that all of us had different views of varying intensity as to just what happened and why. He seemed mollified." Memorandum for the Director, Untitled, December 26, 1962, CREST, NARA.

67. The CIA did not follow Bundy's injunction, on the grounds that it was the "Director's report [to PFIAB] and not a report of the entire administration." After reading it, Bundy reported to Marshall Carter that he thought "it was a pretty adequate job . . . [although] there were a number of places where he [Bundy] might have phrased things differently." Ibid.

68. Roger Hilsman, *To Move a Nation: The Politics of Foreign Policy in the Administration of John F. Kennedy* (Garden City, NY: Doubleday, 1967). The book was controversial because "kiss 'n' tell" memoirs, which unilaterally revealed classified information, had not yet become commonplace.

69. Hilsman, *To Move a Nation,* p. 188.

70. Ibid., p. 187.

71. Ibid. It's instructive to compare *To Move a Nation* with Hilsman's later treatment of the same subject in *The Cuban Missile Crisis: The Struggle Over Policy* (Westport, CT: Praeger, 1996). When this later volume appeared, previously classified information about the September 10 decision had been made public, leaving Hilsman little choice but to change his account. In contrast to his 1967 characterization, in 1996 Hilsman wrote, "there is no evidence of any attempt by the policy makers to suppress information or to hamper intelligence-gathering activities, except for Dean Rusk's *suggestions* [emphasis added] that the U-2 make peripheral flights around Cuba and only for special reasons actually 'dip into' Cuban airspace. But his motive was mainly to avoid a diplomatic brouhaha that might prevent any further U-2 flights, as happened after Gary Powers was shot down. No request from the intelligence community." Hilsman, *Missile Crisis,* p. 55.

72. Hilsman, *To Move a Nation,* p. 196. As pointed out earlier, an exhaustive 1964 CIA study found that the missiles were subject to being detected by U-2 photo coverage any time after September 17–18, weeks before they were actually discovered. To bolster his unprovable assertion, Hilsman engaged in some legerdemain. The former INR director wrote that the SGA lifted the ban on flying over known SAM positions in western

Cuba on October 4, when in fact the Special Group and the president had not made this decision until October 9. By moving up the date, Hilsman made it appear as if the administration had acted with alacrity after receiving new human intelligence reports alleging the presence of large missiles in that region. In fact, even after these reports percolated to the top, the State Department had argued in early October against resuming U-2 flights over known SAM sites, and discovery of the SSMs was postponed by at least an additional five days. Holland, "Photo Gap," pp. 24–26.

73. Hilsman chided the intelligence community for missing other signs of the missile deployment, such as the fact that two Soviet freighters, the *Omsk* and the *Poltava,* had exceptionally large hatches and rode "high in the water" because they were carrying a bulky but relatively light load. "It is difficult to understand why the professional intelligence technicians down the line failed to see enough significance in these facts to bring them to the attention of the top levels." He also deceptively asserted a U-2 could have been dispatched sooner and guided over suspected sites if the CIA had had "a better network of traditional agents" in Cuba. The "intelligence community should have . . . turned their attention to the western end of the island some ten days to two weeks sooner than it did," thereby leaving the inference, for anyone who insisted there was a photo gap, that any delay was primarily the CIA's fault. Hilsman, *To Move a Nation,* pp. 186–87, 189, 191.

74. USIB Report, p. 74.

75. The language quoted is from what appears to be the sixth draft of the USIB Report, and uses the handwritten changes that were presumably incorporated in the seventh draft. The original language of the sixth draft stated, "[B]ut this delay was not critical, because photography obtained prior to about 17 October would not have been sufficient to warrant action or to solicit support from Western Hemisphere or NATO allies." Ibid, p. 89. Presumably the wording was changed because this formulation was at odds with the facts, that is, photo coverage from October 14 had been sufficient to "warrant action."

76. At a meeting of the National Security Council on October 22, Robert Kennedy raised the issue of the photo gap and, in effect, laid down what would be the administration's position. The fact that there had been a delay would be obfuscated, and attributed whenever possible to adverse weather. Indeed, the administration would misleadingly claim that it had *increased* the number of U-2 flights in September. The bottom line, as enunciated by the attorney general, was that "even if there had been U-2 flights, construction at the missile sites was not far enough along to have been detected by photography much earlier than October 14." "Minutes of the 507th Meeting of the National Security Council," October 22, 1962, *FRUS,* Vol. XI, p. 154, and Document 370, "Memorandum of Meeting of Executive Committee of the NSC," October 23, 1962, *FRUS,* Vol. XI, Microfiche Supplement.

77. Because the IG report is still classified, of course, this observation is somewhat speculative.

78. Introducing the element of exactly when the photographs might prove persuasive to NATO and Latin American allies—that is, nonexperts in the detection of SSM sites—was not a trivial matter. But it did not have a great bearing on the issue at hand either. The photos from October 14, which NPIC took as conclusive proof of offensive missile sites, were not the ones shared with U.S. allies. Photos taken days later, deemed to be more revealing to the untrained eye, were shared instead.

79. In light of what later came to be understood as an extensive "denial and deception" program by the Soviets, Earman's report, interestingly, observed that "any post-mortem . . . must take into account whether there was a planned Soviet deception program to help cover their activities. There is little hard evidence on this pro or con, and may never be unless there is a knowledgeable Soviet defector." USIB Report, p. 42, and James Hansen, "Soviet Deception in the Cuban Missile Crisis," *SII* 46 (2002).

80. USIB Report, p. 42.

81. In March 1963 the State Department would attempt to claim, despite Hilsman's participation at every stage, that the USIB post-mortem was not a "coordinated report" but McCone's "personal report," and tried to distance itself from the findings. U. Alexis Johnson, Memorandum for the Honorable John A. McCone, "U-2 Overflights of Cuba, 29 August through 14 October 1962," March 6, 1963; and Memorandum for Director of Central Intelligence, "Department of State's Objections to the Report on the Cuban Arms Build-up," March 12, 1963, both in CREST, NARA.

82. "McCone, Memorandum for the President, 28 February 1963," in McAuliffe, ed., *CIA Documents,* p. 373; Clark Clifford with Richard Holbrooke, *Counsel to the President* (New York: Random House, 1991), p. 357.

83. The USIB Report was formally called the "Report to the President's Foreign Intelligence Advisory Board . . . by the Director of Central Intelligence," in deference to McCone's role as DCI and USIB chairman. But, as shown, the report more genuinely represented the coordinated view of USIB principals than McCone's individual view.

84. Clifford, *Counsel,* p. 353.

85. Ibid., p. 354.

86. George Kistiakowsky, *A Scientist at the White House: The Private Diary of President Eisenhower's Special Assistant for Science and Technology* (Cambridge: Harvard University Press, 1976), p. 21. In one widely publicized incident, McCone, a Caltech trustee, accused some Caltech scientists in 1956 of being taken in by Soviet propaganda when they came out in support of a nuclear test ban. Chalmers Roberts, "McCone Selection Criticized by Some," *Washington Post,* October 23, 1961.

87. Ibid.

88. According to RFK's oral history, Killian declared his vigorous opposition to McCone's appointment. "McCone had made a lot of enemies. [Killian] said he was going to put out a report against John McCone," Kennedy recalled in 1964. "I had to call him and had a long conversation with him. . . . We finally got it straightened out." Edwin Guthman and Jeffrey Shulman, eds., *Robert Kennedy in His Own Words: The Unpublished Recollections of the Kennedy Years* (New York: Bantam Press, 1988), pp. 253–54.

89. U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 94th Congress, 1st Session, *Hearings: Covert Action,* December 4–5, 1975 (Washington, DC: U.S. Government Printing Office, 1976), pp. 50–51.

90. A member of the transition team in 1960, Clifford had already been given his pick of several Cabinet posts by the president-elect in 1960, but he preferred to profit handsomely from his connections to the first Democratic White House in eight years. As Kennedy quipped, Clifford wanted nothing for his services "except for the right to advertise the Clifford law firm on the back of the one-dollar bill." Robert Dallek, *An Unfinished Life: John F. Kennedy, 1917–1963* (Boston: Little, Brown, 2003), p. 306.

91. Clifford, *Counsel,* p. 354.

92. Letter, Clark Clifford to President Kennedy, October 25, 1961, with attachment, "Memorandum on Central Intelligence Agency," in Senate Select Committee, *Hearings: Covert Action,* pp. 139–43. Clifford's 1961 memo, interestingly, advocates that the new DCI operate like the recently created post of Director of National Intelligence (DNI).

93. "Clifford Named to Killian Post," *New York Times*, April 24, 1963. The other PFIAB members in 1962–63 were William Baker, then director of research at Bell Laboratories; Air Force Brigadier General (Retired) James Doolittle; Gordon Gray, a special assistant for national security during the Eisenhower administration; Dr. Edwin Land, an inventor and physicist; Dr. William Langer, a Harvard history professor; former ambassador Robert Murphy; and Frank Pace Jr., secretary of the Army during the Truman administration.

94. Clifford, *Counsel,* p. 354.

95. PFIAB was well aware of McCone's prediction. On September 28 the DCI had discussed Cuba with the panel at some length, and in the context of the charges being made by Senator Kenneth Keating (R-NY) and other congressional critics of the administration's policy. McCone told PFIAB members the same thing he had been telling everyone holding an official position: Although his own analysts disagreed, he believed the Soviets would eventually deploy SSMs in Cuba. Ibid., p. 357.

96. Ibid., p. 355.

97. Ibid., p. 357.

98. "Although the matter was delicate," wrote Clifford, "I felt it was our responsibility to bring our views to Kennedy's attention—especially since his critics were publicly charging him with a failure to act on their early warnings." Ibid.

99. Memorandum for the Record, "DCI Meeting With PFIAB, 7 December 1962," December 10, 1962, CREST, NARA. Access to the Lehman Report, in all likelihood, provided some of the basis for Clifford's early recognition that PFIAB was going to face a "dilemma."

100. Insofar as Helms was concerned, this piece of intelligence was the only "positive and productive" aspect of Operation MONGOOSE. Ted Shackley with Richard Finney, *Spymaster: My Life in the CIA* (Dulles, VA: Potomac Books, 2005), p. 63.

101. Memorandum for the Record, "DCI Meeting with PFIAB, 7 December 1962," December 10, 1962, CREST, NARA.

102. Ibid.

103. The honeymoon cables referred to the telegrams sent to and from McCone while he was vacationing on the French Riviera in September. The DCI had remarried in August, following the death in late 1961 of his first wife.

104. Ibid.

105. The exact moment when McCone learned about the attenuation of U-2 surveillance remains vague to this day. He certainly protested the lack of photo coverage once he returned from the French Riviera in late September. Holland, "Photo Gap," pp. 22–24.

106. Memorandum for the Record, "DCI Meeting with PFIAB, 7 December 1962," December 10, 1962, CREST, NARA.

107. Clifford, *Counsel,* p. 357.

108. Ibid.

109. There probably was a marked difference between having McCone in Washington and receiving McCone's cables from the French Riviera. Nonetheless, as Sherman Kent, chairman of the CIA's Board of National Estimates later observed, even if McCone

"had been in Washington and made a federal case of his intuitive guess, and had got[ten] the President's ear, McCone would have had opposing him (1) the members of USIB, and (2) most presidential advisors including the four most important ones—[former Ambassador Charles] Bohlen, [former Ambassador Llewelyn] Thompson, [former Ambassador George] Kennan, and [serving Ambassador] Foy [Kohler]." All four Kremlinologists were "honest and decent enough" to confirm for Kent in 1971 that they had agreed completely with the September SNIE. Jack Davis, "Sherman Kent's Final Thoughts on Analyst-Policymaker Relations," Sherman Kent Center for Intelligence Analysis, Occasional Papers: Volume 2, Number 3.

110. Clifford also found the September 19 SNIE "preposterous" because, at that exact moment, the DCI was "predicting the opposite." Clifford, *Counsel,* p. 358.

111. Ibid., p. 357.

112. Ibid., p. 358.

113. Though wide of the mark, the Republicans' charge reflected widespread confusion—aided and abetted by the administration—over why the missiles had been discovered belatedly. Holland, "Photo Gap," pp. 28–29.

114. Clifford, *Counsel,* p. 358.

115. Clifford, of course, denied that his position was primarily political. "[M]y major objective, expressed repeatedly in PFIAB meetings, was to strengthen the intelligence efforts in any future crises." Ibid.

116. President's Foreign Intelligence Advisory Board, "Memorandum for the President," December 28, 1962, CREST, NARA.

117. Memorandum for the Record, "Meeting With the President in Palm Beach, Florida," January 7, 1963, *FRUS,* Vol. XI, pp. 651–52.

118. Ibid., p. 651.

119. Ibid., p. 652; Kent, "A Crucial Estimate Relived," *SII* (Spring 1964).

120. Clifford, *Counsel,* p. 355.

121. Ibid. Notwithstanding Clifford's account, the cover page of the final PFIAB report, signed by Dr. Killian, expressed appreciation for the "cooperation and assistance which was freely and promptly given." "PFIAB Memorandum for the President, 4 February 1964," in McAuliffe, ed., *CIA Documents,* p. 361.

122. The meeting was secretly recorded by President Kennedy, but neither the recording nor a transcript of the PFIAB meeting is yet available. See http://www.jfklibrary.org/pres-recordings_available.html.

123. "PFIAB Memorandum for the President, 4 February 1963," in McAuliffe, ed., *CIA Documents,* p. 363.

124. Ibid., p. 364.

125. Ibid.

126. Ibid., p. 365. It may be that this was one of the points on which Clifford and McCone allegedly clashed regarding PFIAB's access to records.

127. Ibid., p. 364.

128. Ibid., p. 365.

129. Richard Helms with William Hood, *A Look Over My Shoulder: A Life in the Central Intelligence Agency* (New York: Random House, 2003), p. 212.

130. Diary Notes, February 21, 1963, CREST, NARA.

131. McCone, "Memorandum for the President, 28 February 1963," in McAuliffe, ed., *CIA Documents,* p. 373.

132. McCone was not going to have the Agency in this position ever again, at least under his watch. In late January he issued a directive ordering Agency personnel "to be very aggressive in taking the initiative to obtain permission for any and all types of intelligence operations to obtain required information for national security." Lyman Kirkpatrick, "Agency Policy on Dynamic Intelligence Operations," January 28, 1963, CREST, NARA.

133. McCone, "Memorandum for the President, 28 February 1963," in McAuliffe, ed., *CIA Documents,* p. 373.

134. Ibid., pp. 373–74.

135. Clifford, *Counsel,* p. 358.

136. Raymond Garthoff, "Documenting the Cuban Missile Crisis," *Diplomatic History* 24 (Spring 2000), p. 300.

137. As pointed out earlier, too, some scholars of the missile crisis, most notably Alexander George and Gil Merom, have been almost as critical.

138. Kennedy, *Own Words,* p. 254.

139. Ibid.

140. Some aspects of the PFIAB post-mortem were simply wrong. The report scored McCone (rather than "higher authority") for imposing the first limitation that "endangered the necessary flow of information" within the intelligence community. "PFIAB Memorandum for the President, 4 February 1963," in McAuliffe, ed., *CIA Documents,* pp. 367, 369; Holland, "Photo Gap," p. 19.

141. The PFIAB report ended with this observation: "Throughout our review, we have been mindful of public charges to the effect that during the period of the Soviet military build-up in Cuba, the U.S. intelligence process was in some manner manipulated for partisan political purposes. We find no evidence whatsoever to support such charges." "PFIAB Memorandum for the President, 4 February 1963," in McAuliffe, ed., *CIA Documents,* p. 371.

142. "Clifford Named to Killian Post," *New York Times,* April 24, 1963.

143. "Cloudy Intelligence," *New York Times,* April 29, 1963.

144. Ibid.

145. Right after the November 1964 election, while discussing possible new appointments, McGeorge Bundy would recall Clifford's PFIAB promotion during a conversation with President Johnson. When Clifford was appointed, Bundy observed, "the *[New York] Times* . . . wrote a very disagreeable editorial saying [we] had replaced a great statesman in Dr. Killian by a Washington fixer named Clifford. Of course, there never were two sillier remarks, because a) Killian was not a great statesman, and b) Clark was just what the doctor ordered, and [did a] judicious job for JFK." Given Bundy's role in the photo gap, he may well have been recalling Clifford's role in the PFIAB post-mortem. Telephone conversation among Bill Moyers, McGeorge Bundy, and Lyndon Johnson, 10:34 am, November 4, 1964, LBJL.

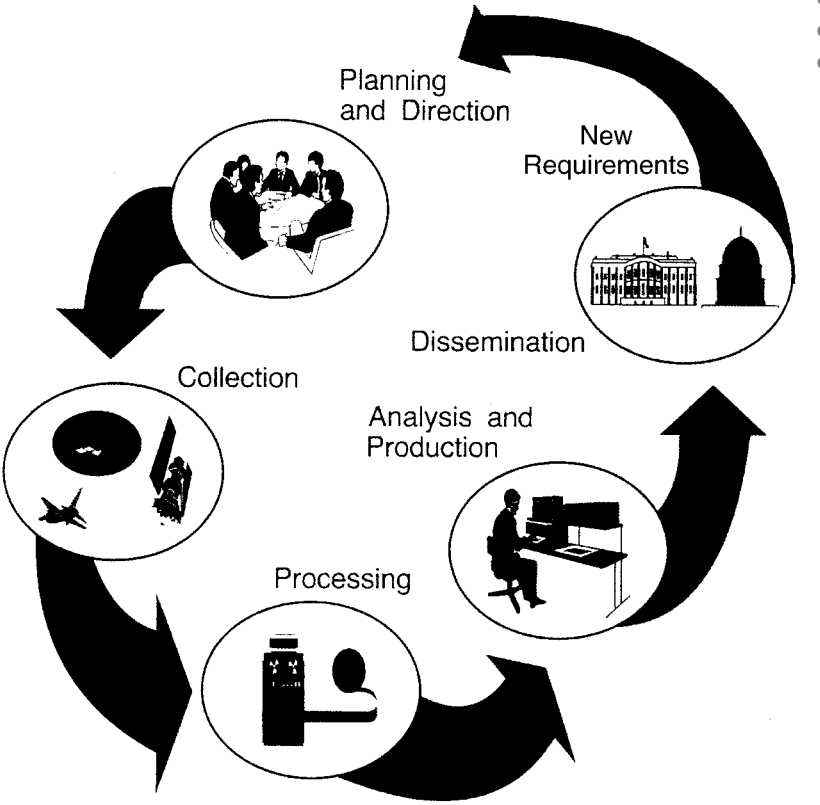
146. Ray Cline, *Secrets, Spies, and Scholars: Blueprint of the Essential CIA* (Washington, DC: Acropolis Books, 1976), p. 197.

147. U.S. Senate, Committee on Armed Services, Preparedness Investigating Subcommittee, *Investigation of the Preparedness Program: Interim Report on the Cuban Military Buildup* (Washington, DC: U.S. Government Printing Office, 1963), p. 8.

148. Richard Shryock, "The Intelligence Community Post-Mortem Program, 1973–1975," *SII* 21 (Fall 1977), p. 27.

APPENDIX A

THE INTELLIGENCE CYCLE



Adapted from *Factbook on Intelligence*, Office of Public Affairs, Central Intelligence Agency (October 1993), p. 14.

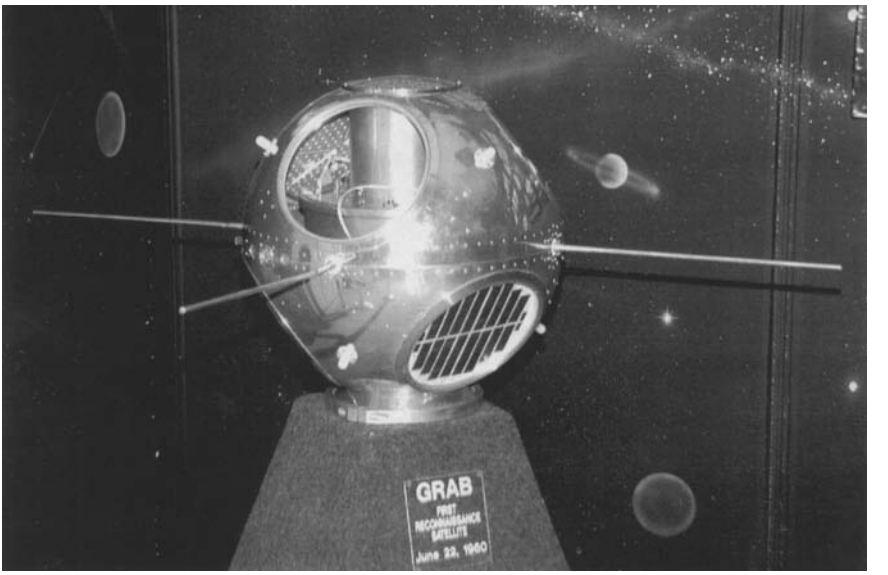
APPENDIX B

EXAMPLES OF AERIAL INTELLIGENCE COLLECTION "PLATFORMS" AND SMALLER COLLECTION DEVICES

A U.S. NAVY RECONNAISSANCE AIRCRAFT, THE EA-30, USED FOR GATHERING ELECTRONIC INTELLIGENCE

Photo courtesy of the CIA Office of Public Affairs, 2006.

THE GRAB II (GALACTIC RADIATION AND BACKGROUND) SATELLITE MODEL



Source: http://www.nsa.gov/museum/museu00027.cfm The GRAB II (Galactic Radiation And Background) satellite was the second Signals Intelligence satellite to be launched by the United States. The first GRAB satellite launched on June 22, 1960, followed the loss of the U-2 spy plane flown by Gary Powers in May. The successful launch of the GRAB II satellite occurred on June 29, 1961. It gathered radar pulses within a specific bandwidth from Soviet equipment. Based on the information NSA received, analysts determined that the Soviets had radars that supported the capability to destroy ballistic missiles. Photo courtesy of the CIA Office of Public Affairs, 2006.

A MINOX TLX CAMERA POPULAR WITH SPIES

Photo courtesy of the CIA Office of Public Affairs, 2006.

U.S. AMBASSADOR TO THE UNITED NATIONS, HENRY CABOT LODGE, JR., REVEALING THE SOVIET PLACEMENT OF AN ELECTRONIC LISTENING DEVICE IN A U.S. EMBASSY SEAL (MAY 26, 1960)

Photo courtesy of the CIA Office of Public Affairs, 2006.

APPENDIX C

EXAMPLES OF IMAGERY INTELLIGENCE FROM RECONNAISSANCE AIRCRAFT AND SURVEILLANCE SATELLITES

TOMSK-7 REACTOR, RUSSIA; U-2 MISSION 4045, 21 AUGUST 1957

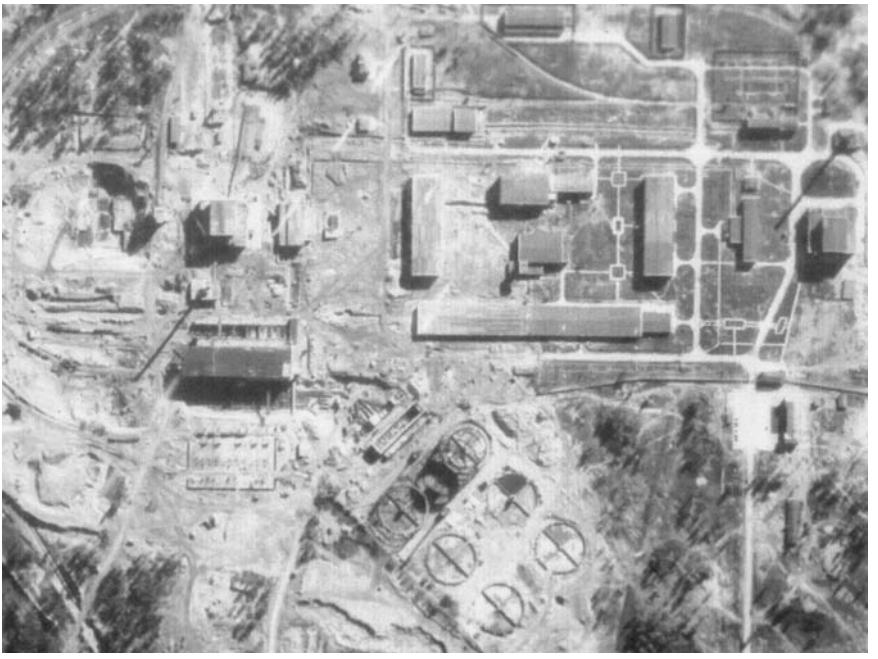


Photo courtesy of the CIA Office of Public Affairs, 2006.

U2 PHOTO OF SOVIET MISSILE SITES IN CUBA, 1962

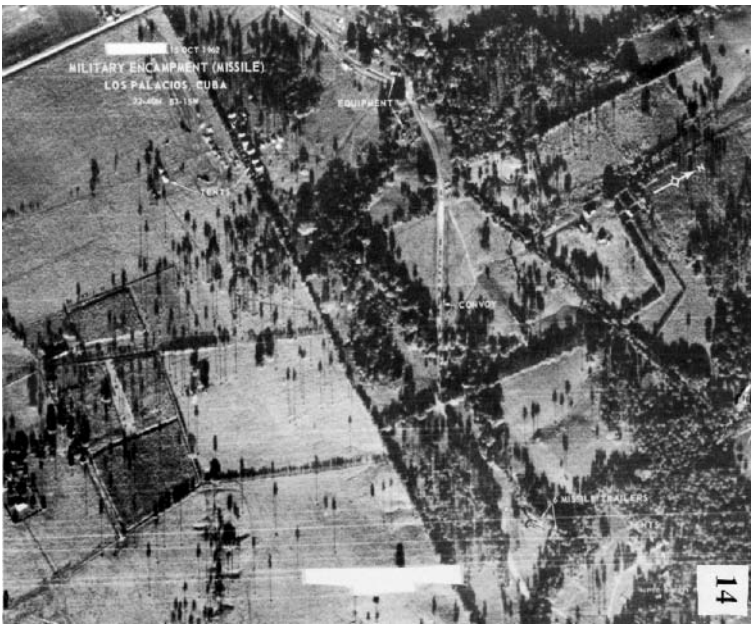


Photo courtesy of the CIA Office of Public Affairs, 2006.

APPENDIX D

CATEGORIES OF FINISHED INTELLIGENCE AND THE MAJOR PRODUCTS

When information that has been reviewed and correlated with information from other sources, it is called "finished intelligence." The five primary categories of finished intelligence are:

1. *Current intelligence* addresses day-to-day events, seeking to apprise consumers of new developments and related background, to assess their significance, to warn of their near-term consequences, and to signal potentially dangerous situations in the near future. Current intelligence is presented in daily, weekly, and some monthly publications, and frequently in ad hoc written memorandums and oral briefings to senior officials.

2. *Estimative intelligence* deals with what might be or what might happen. Like all kinds of intelligence, estimative intelligence starts with the available facts, but then it migrates into the unknown, even the unknowable. The main roles of estimative intelligence are to help policymakers navigate the gaps between available facts by suggesting alternative patterns into which those facts might fit and to provide informed assessments of the range and likelihood of possible outcomes. Such intelligence is promulgated in forms ranging from oral briefings to videos, but the most common vehicles are printed documents, of which the IC's flagship is the National Intelligence Estimate.

3. *Warning intelligence* sounds an alarm or gives notice to policymakers. It connotes urgency and implies the potential need for policy action in response. Warning includes identifying or forecasting events that could cause the engagement of US military forces, or those that would have a sudden and deleterious effect on US foreign policy concerns (for example, coups, third-party wars, refugee situations). Warning analysis involves exploring alternative futures and low probability/high impact scenarios. The National Intelligence Officer (NIO) for Warning serves as the DCI's and the IC's principal adviser on warning. All

---

Source: *Intelligence: A Consumer Guide to Intelligence,* Office of Public Affairs, Central Intelligence Agency (Washington, DC, no date, but made available in the mid-1990s).

agencies and intelligence staffs have designated warning components, and some have specific warning responsibilities:

- NSA maintains the worldwide CRITIC system for the simultaneous alerting of US officials within minutes of situations that may affect US security.
- DIA manages the Defense Indications and Warning System (DIWS) to provide accurate and timely warning of developing threats to US and Allied military interests. Other members include the Combatant Commands, the military services, NSA, State Department/INR, the NIO for Warning, and a growing number of US Allies. DIWS disseminates warning information from DIA and other system members via briefings, weekly and quarterly warning products, and, on a priority basis, ad hoc bulletins.

4. *Research intelligence* is presented in monographs and in-depth studies by virtually all agencies. Research underpins both current and estimative intelligence; there are also two specialized subcategories of research intelligence:

- *Basic intelligence* consists primarily of the structured compilation of geographic, demographic, social, military, and political data on foreign countries. This material is presented in the form of maps, atlases, force summaries, handbooks, and, on occasion, sandtable models of terrain. The Directorate of Intelligence in CIA, NIMA, and the Directorate for Intelligence Production in DIA are major producers of this kind of material.
- *Intelligence for operational support* incorporates all types of intelligence production—current, estimative, warning, research, scientific and technical; it is tailored, focused, and rapidly produced for planners and operators. The top priority of DIA is to satisfy the intelligence needs of operational forces and their commanders. DIA also provides near-real-time intelligence to military forces in peacetime, crisis, contingency, and combat operations. To accomplish this, it operates the Joint Worldwide Intelligence Communication System (JWICS) and deploys National Intelligence Support Teams (NISTs) as needed, worldwide. The Associate Director of Central Intelligence for Military Support, via CIA's Office of Military Affairs, oversees deployment of CIA components of NISTs.

5. *Scientific and technical intelligence* includes information on technical developments and characteristics, performance, and capabilities of foreign technologies including weapon systems or subsystems. This information is derived from analysis of all-source data, including technical measurements. Generally, such technical analysis and reporting responds to specific national requirements derived from the weapons acquisition process, arms control negotiations, or military operations. It covers the entire spectrum of sciences, technologies, weapon systems, and integrated operations. This type of intelligence is provided to consumers via in-depth studies, detailed system handbooks, executive summaries, focused assessments and briefs, and automated databases.

APPENDIX E

SAMPLE NIES ON THE SOVIET UNION AND SNIES ON CUBA AND VIETNAM

NATIONAL INTELLIGENCE ESTIMATE NUMBER 11-6-55
(Supersedes SNIE 11-8-54)

PROBABLY INTELLIGENCE WARNING OF SOVIET ATTACK ON THE US THROUGH MID-1958

Submitted by the
DIRECTOR OF CENTRAL INTELLIGENCE

The following intelligence organizations participated in the preparation of this estimate: The Central Intelligence Agency and the intelligence organizations of the Departments of State, the Army, the Navy, the Air Force, The Joint Staff, the Atomic Energy Commission, and the National Security Agency.

Sources: The 1955 National Intelligence Estimate (NIE) on the Soviet Union, as well as the 1960 NIE on "Main Trends in Soviet Capabilities and Policies, 1960–1965," both stamped TOP SECRET originally, were declassified and released by the Historical Review Program, Central Intelligence Agency (Washington, DC: June 30, 1993; see Donald P. Steury, *Intentions and Capabilities: Estimates on Soviet Strategic Forces, 1950–1983,* CIA History Staff, Center for the Study of Intelligence, Washington, DC, 1993); the September 1962 Special National Intelligence Estimate (SNIE), written on the eve of the Cuban missile crisis and excerpted here, is from Mary S. McAuliffe, ed., CIA Documents on the Cuban Missile Crisis, CIA History Staff (October 1992), pp. 91–93; the SNIE on the situation in South Vietnam in October 1964, just two months after lawmakers approved the Gulf of Tonkin Resolution, and the NIE on "South Vietnam: Problems and Prospects," written in 1971, are both from the National Intelligence Council, Estimative Products on Vietnam, 1948–1975, NIC 2005–03 (April 2005), pp. 288–237, 575–593.

Concurred in by the
INTELLIGENCE ADVISORY COMMITTEE

On 1 July 1955. Concurring were the Special Assistant, Intelligence, Department of State; the Assistant Chief of Staff, G-2, Department of the Army; the Director of Naval Intelligence; the Director of Intelligence, USAF; the Deputy Director for Intelligence, The Joint Staff; and the Atomic Energy Commission Representative to the IAC. The Assistant to the Director, Federal Bureau of Investigation, abstained, the subject being outside of its jurisdiction.

CENTRAL INTELLIGENCE AGENCY DISSEMINATION NOTICE

1. This estimate was disseminated by the Central Intelligence Agency. This copy is for the information and use of the recipient indicated on the front cover and of persons under his jurisdiction on a need to know basis. Additional essential dissemination may be authorized by the following officials within their respective departments:

a. Special Assistant to the Secretary for Intelligence, for the Department of State
b. Assistant Chief of Staff, G-2, for the Department of the Army
c. Director of Naval Intelligence, for the Department of the Navy
d. Director of Intelligence, USAF, for the Department of the Air Force
e. Deputy Director for Intelligence, Joint Staff, for the Joint Staff
f. Director of Intelligence, AEC, for the Atomic Energy Commission
g. Assistant to the Director, FBI, for the Federal Bureau of Investigation
h. Assistant Director for Collection and Dissemination, CIA, for any other Department or Agency

2. This copy may be retained, or destroyed by burning in accordance with applicable security regulations, or returned to the Central Intelligence Agency by arrangement with the Office of Collection and Dissemination, CIA.

3. When an estimate is disseminated overseas, the overseas recipients may retain it for a period not in excess of one year. At the end of this period, the estimate should either be destroyed, returned to the forwarding agency, or permission should be requested of the forwarding agency to retain it in accordance with IAC-D-69/2, 22 June 1953.

This document has been approved for release through the HISTORICAL REVIEW PROGRAM or the Central Intelligence Agency

DISTRIBUTION:

White House
National Security Council
Department of State
Department of Defense
Foreign Operations Administration
Operations Coordinating Board
Atomic Energy Commission
Federal Bureau of Investigation

PROBABLE INTELLIGENCE WARNING OF SOVIET ATTACK ON THE US THROUGH MID-1958

THE PROBLEM

To estimate the probable degree of advance warning that could be provided by intelligence in the event of Soviet attacks on the United States and key US installations and forces overseas through mid-1958.[1]

INTRODUCTION—THE NATURE OF WARNING

When discussing the advance warning of Soviet attack which intelligence may be able to provide, it is necessary to define various possible kinds of warning:

1. Warning of the increased likelihood of war, probably resulting either from Soviet actions or Soviet reactions to Western actions, but not necessarily involving any direct military aspect;
2. Warning of increasing Soviet military readiness to attack, but without definitive evidence of intent to attack or of the time of attack;
3. Warning of clear intent to attack;
4. Warning of clear intent to attack at or about a particular time.

It seems improbable that stage 4, or possibly even stage 3, would be reached conclusively except in the event of high level penetration of the Soviet command, which today seems unlikely, or in case of some exceptional intelligence bonus or breakthrough. While intelligence might be able to say that the USSR would be fully prepared to attack within, say 10 days, it would find it very difficult to say whether such preparations indicated a firm intent to attack, were primarily in anticipation of an expected US attack, were a deception maneuver, or were to prepare against any contingency. When we speak of degree of warning, therefore, it is important to bear in mind that both time and specificity are involved, and that the earlier the warning the less specific it is likely to be. This inverse relation between time and specificity is an inherent limitation of the warning function.

The fact that warning is likely to be in some degree imprecise or contingent also gives increased importance to other considerations affecting the warning function. Both the nature and degree of warning which can be obtained will always be dependent on many complex factors, some of them unique to any given set of circumstances. Warning will depend first of all on maximum alertness and a maximum scale of continuous effort by intelligence. These would probably be maintained only in a period of rising tension and might be reduced, even unwittingly, if the tension ceased to rise, if there were intermittent periods of apparently declining danger, or if intelligence had previously given false warnings. The effectiveness of warning also depends on the continued credibility of intelligence warnings to responsible officials, for warning as a process is complete only when it is acted upon. The warning process is thus affected by the whole context of events in which it operates, including psychological

[1] Since the Soviet attack on the US would be tantamount to general war, this estimate also deals with the over-all warning which the US would be likely to receive of Soviet initiation of general war. It does not consider the warning likely to be given by US or allied early-warning radar, nor the warning which could be obtained from a Soviet ultimatum, since such warning is outside the scope of the problem.

factors and even pure chance. It cannot be regarded as a mechanical process which it is possible for intelligence to set up once and for all and which thereafter operates automatically.

CONCLUSIONS

1. We believe that a Soviet initiation of general war by attacks on the US, its allies, or key overseas installations would almost certainly be preceded by heightened political tension. While such tension would in itself constitute warning that war was becoming more likely, the indications of Soviet preparations which would probably be obtained could be interpreted as evidence of preparations for defense or as part of a war of nerves. Therefore, Soviet behavior in a period of heightened political tension would not necessarily give specific warning of a Soviet intention to attack. Nevertheless, intelligence could probably give warning of the USSR's increasing war readiness and could probably chart the trend toward a period of maximum danger. *(Paras. 12–15, 18)*

2. It would also be possible for the Soviet leaders, after a period of prolonged tension in which they had brought both their political and military preparations to an advanced stage, to bring about an amelioration of the crisis atmosphere as a deception move. Such a move, while involving sacrifice of some advantages, would almost certainly be made if the Soviet leaders considered that a maximum degree of surprise was essential to their strategic plans. Allied intelligence, however, might still be able to detect the continuation of specific military preparations which would be particularly significant as evidence of a Soviet intention to achieve surprise in launching general war. *(Paras. 16–17)*

3. If the USSR chose to initiate war with full-scale land, naval, and air attacks after a period of mobilization, there would be numerous indications of military, as well as of economic and political measures necessary to prepare such attacks. We believe that US intelligence might be able to give a generalized degree of warning as long as four or possibly even six months prior to D-Day, and that the minimum period would not be less than 30 days. After D-30 the number of indications would probably be reduced due to Soviet security measures, although the latter would themselves provide warning. From D-10, and especially D-5, there would probably be certain indications of last-minute preparations, although processing and disseminating these on a timely basis would probably be difficult. As the time of attack drew near, indications of its approach would become increasingly specific. Based on observed Soviet military activities, warning could probably be given from a few hours to a few days in advance of the actual launching of the attack. (*Paras. 21–25)*

4. In order to gain some degree of surprise, the USSR might choose to initiate general war by attacks of less than full scale in Europe, the Middle East, or in the Far East directly or through the Chinese Communists, while simultaneously attacking the US and key overseas installations. The degree of prior Soviet preparations would vary greatly, depending on the location of the attack and the intensity and direction of the preceding political tensions. Even so, the minimum preparations which the USSR would have to take to put its forces in a state of readiness to attack, and to provide support after the attack began would probably require about 15 days. We believe that warning of the probability of attack could be given about one week in advance, but the period might vary from a few hours to as much as 10 days, depending on the seasonal pattern of Soviet military activity. *(Paras. 27–28)*

5. We have estimated in NIE 11-7-55 that by exercising its maximum capability the USSR could now launch about 950 bomber aircraft against the US in an initial attack. However, virtually all of these aircraft would be medium bomber types (BULLS and BADGERS); a few would be heavy bombers (BISONS and BEARS). The great bulk would

have to fly one-way missions. At present, Soviet preparatory activities for maximum scale attack would require at least several months, and probably considerably longer, and would probably become known to allied intelligence, especially if carried forward with great urgency. We believe that the indicators would probably assume a meaningful pattern in time for intelligence to give a generalized degree of warning 15–30 days prior to attack. US intelligence would also be likely to discover significant activities indicating the movement of the large numbers of aircraft to staging bases involved in such a maximum scale attack. We believe that intelligence could give specific advance warning of unusual and possibly threatening air activity on the order of 18–24 hours.[2] *(Paras.* 35–38)

6. We have estimated in NIE 11-7-55 that if the USSR attempted a surprise attack against the US in 1955, aircraft would probably be launched from 11 available staging bases in the Kola, Chukotski, and Kamchatka areas.[3] There is a lack of sufficient evidence to permit a firm assessment of the capabilities of the individual bases in these areas for staging bomber aircraft. However, we believe that by a major effort the USSR could launch some 450 aircraft on initial attack against the US. Preparations for such an attack would permit possible detection by allied intelligence and, if detected, would provide a generalized degree of warning of several days, and specific advance warning of unusual and possibly threatening air activity on the order of 18–24 hours. *(Para. 42)*

7. A reduced scale of attack, however, involving about 250 aircraft could be launched against the US and, accompanied by an extraordinary security effort, might be launched in 1955 with little or no specific advance warning to US intelligence. This estimate rests on the belief that the forward bases may now be capable of handling these aircraft or may become so without detectable preparations. (Para. *43)*

8. By 1958 the bases, training, and equipment of the Soviet Long-Range Air Force could, by a major effort, be advanced to a point where only minimum preparations would be required prior to a maximum attack which could then number about 1,100 bomber aircraft. Provided that such a major effort has been made, movements in and out of the forward staging bases may also become routine. The likelihood that these movements would be discovered would not be much less than at present, but the difficulty of assessing them as warning indicators would thus be very much greater. Moreover, by 1958, the increased speeds of jet bombers will reduce the time required for movement to staging bases and the probable increased handling capabilities at the bases will reduce time required for refueling and servicing. Consequently the specific advance warning of unusual and possibly threatening air activity which could be given, assuming that movement to the staging bases was discovered and correctly interpreted, would probably be on the order of 12–18 hours.[4] *(Para. 39)*

---

[2] Here and in paragraphs 6, 8, and 9 warning given in hours is defined as the elapsed time between the receipt of information (by a US command or agency having authority to alert US defenses) which indicates threat of a possible imminent Soviet air attack, and the time such an attack would reach the existing continental early warning line (1955) and the proposed (DEW) line (1958).

[3] For a full discussion of these forward bases, see NIE 11-7-55, "Soviet Gross Capabilities for Attacks on the US and Key Overseas Installations and Forces through 1 July 1958."

[4] The Director of Intelligence, USAF, believes that movement in and out of forward staging bases may become routine by 1958 if currently indicated efforts to improve the bases, training, and equipment of the Long-Range Air Force continue. He also believes it unlikely that such movement would be discovered and correctly interpreted before its value as warning had passed. Moreover, the increased capability of the Soviet Union to launch heavy bombers from interior bases will further degrade this source of warning information.

9. Both at present and in 1958, if the movement to staging bases was not discovered, warning could be obtained only if almost continuous reconnaissance of the staging areas was being maintained and aircraft were discovered after they had already reached these areas. However, reliance on this means alone might reduce the warning period to a few hours, or even virtually to zero, because of possible difficulties and delays in processing and interpreting the results of the reconnaissance. *(Para. 40)*

10. During the period of this estimate the USSR will have a progressively increasing capability for launching one-way attacks on the US from interior Soviet bases which would probably provide no specific advance warning to US intelligence.[5] Moreover, there are two other ways by which the USSR might by 1958 (and possibly somewhat before that year) launch an attack on the US in such a way that no specific warning would be likely before its actual launching:

a. Assuming that the USSR pressed ahead with development of its advance bases in the Chukotski, Kamchatka, and Kola areas, and with the general preparation of its Long-Range Air Force, "normal" flights of aircraft to and from these bases would almost certainly occur in increasing number as the development of the bases progressed. A pattern of activity would thus tend to be established. Under these circumstances, a considerable number of aircraft—roughly the number engaging in such "normal"activity—would almost certainly be able to take off from these bases (and those in the Leningrad area) for a surprise attack upon the US without any such unusual prior preparations or assembly as would particularly attract the attention of allied intelligence.

b. Assuming that the USSR acquires an inflight refueling capability (which it can do although there is no evidence at present that the Soviet Long-Range Air Force possesses such a capability) and develops it to the necessary degree, Soviet heavy bombers could also be launched on two-way missions from certain home bases without specific advance warning, and without staging at the advance bases.[6] *(Paras.* 35, 45)

11. If the USSR, concurrently with any of the scales of attack discussed above, undertook submarine operations against the US and key overseas installations, it would be necessary for the submarines so employed to proceed to wartime patrol stations shortly before the expected commencement of hostilities. The passage of these submarines might give up to two weeks warning of Soviet preparation for attack. If the USSR undertook concurrent raider operations with some of the major units of their surface fleet against allied lines of communication, the movement of these raiders might give up to 10 days warning of preparation for attack. *(Paras. 30–31)*

12. Soviet preparations to receive a retaliatory blow from allied air power could probably provide some indication of Soviet intent to attack. Minimum preparations would probably include the alerting of air defense forces and the civil defense organization, preparations of military units and installations for air defense, the dispatching of submarines accompanied by increased aerial reconnaissance to locate US carrier forces, and the evacuation of key personnel and possibly segments of population from potential target areas. If steps such as these were taken, they would probably provide a warning period of as much as a week to 10 days, and, taken in conjunction with other indicators, would

[5] For full discussion of Soviet long-range capabilities, see NIB 11-7-55, "Soviet Gross Capabilities for Attacks on the US and Key Overseas Installations and Forces through 1 July 1958."

[6] Only the BEAR (Turbo-prop), with its tentatively estimated characteristics, could reach all targets in the US. See NIE 11-7-55.

greatly increase the definiteness of any warning US intelligence might be able to give. We believe that in elementary prudence the USSR would be unwilling to forego preparation to receive a retaliatory blow; therefore, some important indicators of this type would probably be obtained. *(Para. 46)*

DISCUSSION

I. Warning From Soviet Behavior in Various Circumstances

13. The various possible circumstances in which the USSR might decide to attack the US and enter upon general war would have a considerable bearing on the degree of warning which might be obtained.

a. There are three situations in which the USSR might deliberately decide to attack the US and key overseas installations, thus initiating general war. These situations would arise if the Soviet leaders came to believe: (1) that the USSR had acquired such military capabilities that it could be certain of success in a general war; (2) that the US and its allies were planning an attack on the USSR and that the USSR's only hope of survival lay in seizing the initiative; or (3) that an irreversible shift in the relative weight of military power was impending which would ultimately force the USSR to choose between certain defeat in war and sacrifice of its vital interests. We believe that the Soviet leaders are unlikely to come to any of these conclusions during the period of this estimate.

b. There remains the possibility that general war might occur after a series of actions and counteractions in some local crisis which neither the USSR nor the Western Allies originally intended to lead to general war. If the USSR believed that the issues at stake were vital to its security or that the loss of prestige involved in backing down would be equally dangerous to Soviet power, and if it believed that the US would not yield, then the USSR might decide that general war was the unavoidable consequence of the crisis and that it should seize the initiative. We believe that if the USSR decides to launch general war in the period through mid-1958, the decision is most likely to come as the consequence of such a situation.[7]

14. *Likelihood of a Period of Tension.* In the situation described under *b.* above, a Soviet decision to attack the US would be preceded by a period of heightened tension. Moreover, even if the Soviet leaders reached any one of the three conclusions in *a.* above, they would probably do so because of an important shift in international alignments, or because of some equally open and marked alteration or impending alteration, of the relative weight of military power. Such developments would themselves be likely to produce heightened political tension. There are situations, however, in which a Soviet decision for war could be taken in the absence of political tension. For example, a Soviet decision motivated as under *a.* (1) above might be the result of some technical advance in Soviet military capabilities unknown to the Western Allies, or a Soviet decision motivated as under *a.* (3) above might be the result of some secret technical advance in Western military capabilities of which Soviet intelligence learned. We believe that such situations are unlikely to arise. Therefore, since an attack on the US, if it occurs, is most likely to

[7] The Soviet attitudes toward general war referred to in paragraph 13 are discussed more fully in NIE-3-55, "Soviet Capabilities and Probable Courses of Action Through 1960," dated 17 May 1955, Sections VI and VII.

arise from a series of actions and counteractions not originally intended to lead to general war (paragraph 13 *b.*), it would almost certainly be preceded by a period of heightened tension.

15. *Reliability of Political Indicators in a Period of Tension.* While the existence of a prior period of tension would in itself constitute warning that war was becoming more likely, it would also greatly increase the difficulty of obtaining from Soviet political behavior a specific warning of attack. Most of the political actions taken by the USSR during a period of war preparation might not differ greatly from those undertaken as routine in any period of heightened political tension. These actions might include: diplomatic approaches to some states designed to influence them toward abandonment of their alliances with the US; massive "peace" propaganda directed at the populations of Western states and intended to undermine the will to resist or to destroy confidence in the motives and intentions of governments; explicit threats against would-be aggressors; new proposals to ban nuclear weapons; instructions to Communist parties to ready themselves for their sabotage and subversion missions; intensified propaganda directed to the Bloc populations to prepare them psychologically for "resistance to aggression." All such actions, however, could be interpreted as defensively motivated or as part of a war of nerves. Thus while they might provide warning of the increased likelihood of general war, they would not provide specific warning of attack.

16. *Reliability of Military Indicators in a Period of Tension.* The existence of a period of heightened tension would also make more difficult the determination from Soviet military preparations of a specific intent to attack. If in such a period the USSR undertook various military preparations, it would probably be as difficult to distinguish offensive from defensive intent as in the case of indicators from Soviet political behavior. In a protracted situation of this sort intelligence probably could only give warning of the USSR's increasing war readiness and chart the trend toward the period of maximum danger, but not warn of a Soviet intention to attack. The USSR might be carrying out military preparations not in order to initiate war but in readiness for instant retaliation to a US attack which it feared might be impending.

17. *Possibility of Soviet Deception.* It would also be possible for the Soviet leaders, after a period of prolonged tension in which they had brought both their political and military preparations to an advanced stage, to bring about an amelioration of the crisis atmosphere as a deception move. They could offer concessions as a basis for new negotiations, and simulate reduction of some of their military preparations, or even actually reduce them. If they considered surprise essential to their plans and believed that they still could achieve some degree of surprise in their initial attack, this would be a likely course for the Soviet leaders to pursue. However, such a course would involve sacrifice of some advantages. An initial surprise assault aimed at Western retaliatory power might include air attacks on the territories of some states which the USSR might otherwise have hoped to neutralize politically. It would probably also involve the clear assumption of responsibility for initiating war by aggressive action, and thus might harden the will to resist in some Western countries. Nevertheless, the Soviet leaders would almost certainly accept these disadvantages and attempt deceptive political maneuvers if they considered that the maximum degree of surprise attainable was essential to their strategic plans.

18. Although a large degree of deception could be introduced into Soviet behavior, allied intelligence might still be able to detect the continuation of specific military preparations. Such indications could be interpreted as due to Soviet caution and mistrust, but they

would also point to the possibility of a deception maneuver and they would be particularly significant as evidence of a Soviet intention to achieve surprise in launching general war.

19. *Summary.* We believe, therefore, that Soviet behavior in a period of heightened tensions would not necessarily give warning of attack. It would probably establish that Soviet readiness for general war was increasing; it would also establish that the likelihood of war was increasing but would not necessarily indicate that general war was probable. It would also lead to heightened activity and sensitivity on the part of allied intelligence. However, neither a belligerent and unyielding attitude nor a defensive and conciliatory one would be a sure guide to Soviet intentions.

II. Alternative Scales of Soviet Attack

20. The probable, degree of warning that the West would receive of Soviet attack would depend in large part upon the type of attack initiated. Many courses of action are open to the Soviet planners in the event they should decide to initiate a general war. At one end of the spectrum would be a massive multifront Soviet attack on the US and allied states, undertaken after a period of intensive mobilization. Such a plan of attack would sacrifice strategic surprise in favor of maximum military preparation, although the USSR might still hope to achieve some degree of tactical surprise. At the other end of the spectrum would be a Soviet surprise attack, with no prior preparations of a nature that could be relied on to provide warning indicators. Such an attack would sacrifice weight for the advantages of surprise. This estimate does not attempt to forecast Soviet strategy or the probable scale of the initial attack. It only discusses the probable degree of warning which would be obtained if Soviet planners selected any one of the following alternatives for their initial attack:

a. Full-scale attack after a period of general mobilization;

b. Soviet campaign in Western Europe from existing deployments and simultaneous attacks on the US and key US overseas forces and installations;

c. Initial attacks only on the US and key US overseas forces and installations

(1) Maximum scale attack

(2) Surprise attack.

III. Warning of Full-Scale Soviet Attack

21. A full-scale attack employing all arms in strength at the outset of war would necessarily be preceded by a period of mobilization during which full war readiness, or a condition close to it, had been achieved. The range of activities necessary for such full mobilization of war potential in a highly industrialized state like the USSR is so extensive and involves so many measures affecting broad sections of the population that even a totalitarian government would find it impossible to conceal all of them. In the economic field, a complex redirection and intensification of productive effort would have to take place as materials, manpower, and facilities were transferred from consumption and investment goods industries to armament industries. These measures would probably be impossible without the use of public information media. In addition, manipulation of domestic opinion is so persistent a preoccupation of the Soviet government and its concern over popular morale under conditions of crisis is so intense that its vast propaganda

apparatus would certainly be openly committed to preparing the Soviet people to withstand the strains of general war.

22. In the military field itself, the induction of additional military classes, formation of new units and fleshing-out of existing units to full strength, intensified and more realistic training, redeployment of combat groups to forward areas, and a variety of logistic measures would hardly escape entirely the observation of Western intelligence. In particular, it would be difficult for the USSR to hide large-scale troop movements in East Germany or the other Satellites and forward deployment of its naval units. Withdrawal of a significant portion of civil aircraft from scheduled flights to augment the aircraft of the airborne forces or for other purposes might give additional warning of full-scale attack. At present numerous specific preparations for a full-scale air effort against the US would have to be made by the Soviet Long-Range Air Force, although by mid-1958 the extent and reliability of such indicators could be considerably reduced (see paragraph 37 below).

23. At present, if the USSR undertook to mobilize for a full-scale attack, US intelligence would probably receive numerous indications of large-scale Soviet mobilization during a period of about six months to about one month before D-Day, largely because the preparations likely to be undertaken during this period would be those least susceptible of concealment. However, if the decision to proceed to full mobilization came after a period of prolonged tension in which preparatory measures were initiated, or if by 1958 general Soviet war readiness should be substantially increased, then initial indicators might appear considerably later than six months prior to D-Day. In any event, from roughly D-30 to around D-10 days, we would be likely to get much less in the way of indications because the preparations in this period would be those which Soviet security is best equipped to conceal. Moreover, by about one month before D-Day the progressive tightening of Soviet security measures would probably have reached a high point. There would almost certainly be a reduction in information from sources within the Bloc; at the same time, however, the drying up of internal Bloc sources because of intensified security measures would in itself provide an indication of Soviet preparations. Then, in the period from D-10 and especially D-5 on, we could expect indications of last-minute preparations. At this time, however, there would be a serious problem of processing and disseminating such indications on a sufficiently timely basis.

24. We believe that allied intelligence would probably be able to sort the variety of indicators into a meaningful pattern at a relatively early stage of Soviet mobilization for a full-scale attack. US intelligence might become aware of this mobilization as long as four or possibly even six months prior to D-Day. The minimum period would probably not be less than 30 days. Even though intelligence was able to give only a generalized degree of warning, showing the progressive increase of Soviet war readiness, it would probably still be able to chart the trend of full-scale preparations, to anticipate their probable course to completion, and thus to designate the beginning of a period of maximum danger. It might even be able to identify features of Soviet full-scale mobilization which because of their uniqueness or extreme costliness could be interpreted specifically as evidence of an intention to attack.

25. As the time of attack drew near, indications of its possible approach would become increasingly specific. Based on observed Soviet military activities, warning could probably be given from a few hours to a few days in advance of the actual launching of the attack. This would be rendered very difficult, however, if Soviet forces, when their preparations for attack were known to be near completion, undertook air, naval, and

ground reconnaissance, or attempted major feints. These activities might provide evidence of Soviet intention to attack, but would aggravate the difficulty of determining the time of such attack. It might also be recognized that, in theory at least, the USSR could always refrain from or delay attacking even after preparations were complete. Hence the indications of military readiness, taken by themselves, would not necessarily provide conclusive evidence that attack was certain.

IV. Probable Degrees of Warning in the Event of Less Than Full-Scale Attack

26. If the USSR were to sacrifice weight for the advantages of surprise, it would be forced, depending upon the degree of suprise it sought, to accept certain major limitations: (a) no large-scale mobilization of additional units; (b) no large-scale redeployment of Soviet air, naval, or ground forces, especially to forward areas; and (c) no unusual movement of Soviet air, naval, or ground forces in such areas as would be likely to indicate the imminence of attack. However, even if the USSR attempted to achieve the utmost surprise in launching general war, it would still probably consider a minimum number of prior preparations a matter of necessity and elementary prudence. Therefore, at least some of the general preparations discussed in Section III above would almost certainly have to be undertaken. Some of these preparations would be detected by allied intelligence, but it probably would be very difficult to ascertain any such clear pattern of preparations as would be discernible in event of mobilization for full-scale attack. Again, the degree of readiness already achieved by Soviet forces would affect the number of indicators obtained and the general political situation would affect the intensity of US intelligence effort and the ability of intelligence to interpret correctly such indicators as it did obtain. Consequently, we believe it possible that these preparations would not lead to a warning of attack, especially if they were carried out over a long period of time and with careful concealment.

27. If the USSR decided to attack the US and key overseas installations without full prior mobilization for general war, and hence without full-scale attacks in other areas, two general alternatives would be open:

a. It could combine its attack against the US and key overseas installations with a surprise ground campaign in Europe, the Middle East, and in the Far East directly or through the Chinese Communists without prior reinforcement of its forces.[8]

b. It could undertake initially air, and possibly other forms of attack, against the US and key overseas installations, but delay its ground campaigns and discernible preparations for other military operations until after these initial attacks had been launched.

V. Soviet Campaign in Major Areas and Simultaneous Attacks on the US and Key Overseas Installations

28. If the USSR chose to initiate general war by an attack with the forces currently stationed in Europe, the Middle East, and the Far East, together with attacks on the US and key overseas installations, the degree of its over-all prior preparations would vary greatly,

[8] The USSR could of course strengthen this ground attack by some degree of prior reinforcement. For the purpose of this estimate, however, we take the above case as the limiting one: i.e., any prior reinforcement would tend to provide additional indicators and hence additional warning.

depending on the location of the attack and the intensity and duration of the preceding political tensions. If, as we think likely, there had been a long period of crisis, the USSR might have already achieved a considerable degree of military and economic mobilization for war, and its foreign and domestic political preparation might be well advanced. Moreover, during the period 1955–1958, measures may be taken ostensibly or actually in response to external developments, e.g., West German rearmament, which would greatly improve Soviet readiness for attack. Therefore, the indicators derived from such activities, though warning of the increased readiness for war and likelihood of war, would probably be of limited significance for warning of this type of attack. Even so, the minimum local preparations which the USSR would still have to take for an attack with forces in place would provide some degree of warning.

29. In Europe, for example, some time would be required to assemble major elements in forward positions, although this would vary seasonally. The longest period required would be between May and August when units are split between home stations and field training areas; a lesser period would be required between November and March when units are consolidated at home stations; the minimum period required would be in April when units are moving to training areas and in September–October when units are either engaged in large-scale maneuvers or are being moved back to home stations. Other minimum preparations would include the release from stocks of transport, munitions, and supplies in quantities well in excess of those used even on full-scale maneuvers. In addition, some two weeks before the attack it would probably be necessary to begin the movement of large numbers of locomotives and rolling stock from East Germany to the Soviet border in order to prepare for resupply and reinforcement operations to support and expand the offensive. Altogether, the USSR would probably be engaged in these preparations over a period of about 15 days and US intelligence would probably begin to acquire some indicators at an early stage, although varying with the season of the year. We believe that warning of the probability of attack could be given about one week in advance. However, in the absence of other indicators and with Soviet actions appearing to be part of a normal pattern, the warning could vary as follows:

a. from a few hours to a few days in April and in September–October;

b. from two to five days in November–March;

c. from five to 10 days in May–August.

30. If the USSR undertook concurrent submarine operations against the US and key overseas installations, it would be necessary for the submarines so employed to proceed to wartime patrol stations shortly before the expected commencement of hostilities. The passage of these submarines might give up to two weeks warning of Soviet preparation for attack.

31. If the USSR undertook concurrent raider operations with some of the major units of their surface fleet against allied lines of communication, it would be necessary for the units so employed to proceed to their assigned areas of operations shortly before the expected commencement of hostilities. The movement of these raiders might give up to 10 days warning of preparation for attack.

32. In addition, any unusual and unexplainable deviation from the normal operating pattern of the Soviet Bloc merchant marine could be a supporting indicator of Soviet preparations to attack.

33. The extent to which the preparations going on simultaneously for air attack on the US and key overseas installations and forces would tend to confirm and/or advance

the warning would depend somewhat upon the planned scale of these attacks, as discussed below.

VI. Initial Air Attacks on the US and Key US Overseas Forces and Installations

34. For the purposes of this estimate it is necessary to consider two types of air attack on the US and key overseas installations: (a) a maximum effort using as many aircraft as possible, and (b) an attack designed to achieve a high degree of surprise. The USSR could undertake these air attacks on the US and key overseas installations and forces simultaneously with a full-scale attack in Eurasia or with the less than full-scale attacks discussed in paragraphs 26–32. Alternatively, the USSR could initiate general war with such air attacks only, while delaying discernible preparations for other military operations in order to increase the likelihood of surprise against the US. In this case, the very disparity between preparations for long-range air operations and those for other general war campaigns could be a highly significant indicator of the probable nature of the initial Soviet attack.

35. *Maximum Air Attack.* We have estimated in NIE 11-7-55 that by exercising its maximum capability the USSR could now launch about 950 long-range aircraft against the US in an initial attack.[9] By mid-1958 the maximum number launched could be increased to about 1,100. However, we believe extensive prior preparations would be required, particularly in the early part of the period covered by this estimate. These would almost certainly include improving airfields, maintenance and fuel storage facilities in the Chukotski, Kamchatka, and Kola areas, bringing personnel and equipment to full strength in long-range air units, probably intensified training of air personnel, increased frequency of long-distance training missions, and raising levels of maintenance, and possibly training in inflight refueling techniques. The critical indicators would be those relating to increased levels of activity at staging bases in the Chukotski, Kamchatka, and Kola areas, since in 1958 as well as at present these bases would be essential to maximum attacks on the US. By 1958, however, the degree of Soviet dependence upon these forward areas, and thus their significance as a warning indicator, would decline if the USSR, as part of a maximum scale attack, chose to launch some or all of its heavy bombers directly from interior bases or either one- or two-way missions or combinations thereof. Except for the BEAR (turboprop), even Soviet heavy bombers employing inflight refueling would still require advanced bases for making two-way attacks on the most distant US targets.

36. At present, Soviet preparatory activities for maximum scale attack would require at least several months, and probably considerably longer, and would probably become known to allied intelligence, especially if carried forward with great urgency. We believe that the indicators associated with preparation of the advance bases, taken together with others pointing to the increased readiness of the Long-Range Air Force, would probably assume a meaningful pattern in time for intelligence to give a generalized degree of warning 15–30 days prior to attack. Nevertheless, this would be warning only of increased readiness and not of intent to attack.

[9] The great bulk of these aircraft would have to fly one-way missions, but the problem of *advance warning* by intelligence, as distinguished from *tactical warning* by early warning radar, would not be significantly different if the USSR, in order to permit two-way missions by more of the strike aircraft, chose to include some proportion of tankers, if available, in the total number of planes launched.

37. If such preparations proceeded gradually over the next few years, they would have even less significance for warning, since they could well be part of a normal build-up of the USSR's long-range air capability. Thus, by 1958, the bases, training, and equipment of the Soviet Long-Range Air Force could be advanced to a point where only minimum preparations would be required prior to an attack. There would then need to be little in the way of movement of personnel and equipment, logistic activity, or training flights which would depart from a normal pattern of activity. Under these circumstances, indicators of the preparations taking place in the Soviet Long-Range Air Force might be few, and warning would depend almost entirely on indicators received during the staging of aircraft.

38. At present, US intelligence would be likely to discover significant activities indicating the movement of the large numbers of aircraft to staging bases involved in a maximum scale attack. Considering also the amount of time that the aircraft would require to reach such bases, together with the time required for refueling and servicing at the bases, we believe that intelligence could give specific advance warning[10] of unusual and possibly threatening air activity on the order of 18–24 hours before the attacking aircraft reached the early warning radar screen. It would always be possible, of course, for such a movement to be a practice maneuver or a feint, and therefore warning of actual intent to attack could not be given with complete certainty.

39. Developments are taking place in the Soviet Long-Range Air Force which probably will decrease the possibility of detection, and increase the difficulty of interpreting indicators in terms of intent to attack. By 1958, movements in and out of forward staging bases may become routine, provided that during the interim a major effort had been undertaken to improve base facilities and training, logistics, and equipment of the Long-Range Air Force. The likelihood that these movements would be discovered would not be much less than at present, but the difficulty of assessing them as warning indicators would be very much greater. In addition, by 1958 the increased speeds of jet bombers will reduce the time required for movements to staging bases, and the probable increased handling capabilities at the bases will reduce time required for refueling and servicing. Consequently, the specific advance warning of unusual and possibly threatening air activity which could be given, assuming that movement to the staging bases was discovered and correctly interpreted, would probably be on the order of 12–18 hours.[11]

40. Both at present and in 1958, if the movement to staging bases was not discovered, warning could be obtained only if almost continuous reconnaissance of the staging areas was being maintained and aircraft were discovered after they had already reached these areas. However, reliance on this means alone might reduce the specific advance warning period to a few hours, or even virtually to zero, because of possible difficulties and delays in processing and interpreting the results of reconnaissance. Moreover, by 1958 the

[10] Here and in paragraphs 39, 40, 42, and 44 warning given in hour terms is defined as the elapsed time between the receipt of information by a US command or agency having authority to alert US defense which indicates an imminent threat of Soviet air attack, and the time such an attack would reach the existing continental early warning line (1955) and the proposed (DEW) line (1958).

[11] The Director of Intelligence, USAF, believes that movement in and out of forward staging bases may become routine by 1958 if currently indicated efforts to improve the bases, training, and equipment of the Long-Range Air Force continue. He also believes it unlikely that such movement would be discovered and correctly interpreted before its value as warning had passed. Moreover, the increased capability of the Soviet Union to launch heavy bombers from interior bases will further degrade this source of warning information.

probable growth in Soviet air defenses would make such reconnaissance considerably more difficult.

41. The additional preparations which would be necessary to attack US overseas installations would not increase the likelihood of specific advance warning.[12] In the event of a maximum scale attack, the long-range air arm would already be in a high state of readiness. The readying of the jet light bomber units which could also be used for attacks in Western Europe, the UK, and some parts of the Middle East and Far East could be accomplished without serious additional risk of detection unless very large numbers had to be deployed to forward bases. If guided missiles were employed, no warning of their use would be obtained, apart from the generalized warning which might have been derived from prior preparations for hostilities.

42. *Surprise Air Attack.* However much the Soviet planners desired to achieve surprise in their initial air attacks on the US and key overseas installations, they would still wish to achieve the optimum weight of attack consistent with surprise. We have estimated in NIE 11-7-55 that if the USSR attempted a surprise attack against the US in mid-1955, aircraft would probably be launched from the 11 available staging bases in the Kola, Chukotski, and Kamchatka areas. There is a lack of sufficient evidence to permit a firm assessment of the capabilities of the individual bases in these areas for staging bomber aircraft. However, we believe by a major effort the USSR could launch some 450 aircraft on initial attacks against the US. Preparations for such an attack would permit possible detection by allied intelligence and, if detected, would provide a generalized degree of warning of several days, and specific advance warning of unusual and possibly threatening air activity on the order of 18–24 hours.

43. A reduced scale of attack, however, involving about 250 aircraft could be launched against the US, and accompanied by an extraordinary security effort, might be launched in mid-1955 *with little or no specific advance warning to US intelligence*. This estimate rests on the belief that the forward bases may now be capable of handling these aircraft or may become so without detectable preparations.

44. As estimated in paragraphs 37 and 38, by 1958 the USSR could, provided forward base construction, training, and equipment of the Soviet Long-Range Air Force were sufficiently developed, launch its maximum air attack of about 1,100 aircraft against the US under such conditions that the period of specific advance warning of unusual and possibly threatening air activity would probably be on the order of 12–18 hours, and might be considerably less if the movement to staging bases was not discovered. Thus in 1958 the maximum Soviet air attack, provided no other warning of Soviet intent to go to war had been received, could achieve a high degree of surprise.

45. During the period of this estimate the USSR will have a progressively increasing capability of launching one-way attacks on the US from interior Soviet bases which would

[12] Although variations in the relative priority as to timing and weight of attack between the US and overseas installations would not affect the *advance warning* obtained by intelligence, they would be of great significance for the *tactical warning* derived from radar due to the varying times at which aircraft bound for targets at different distances would be picked up. For example, if the USSR chose to make attacks on overseas installations before launching attacks on the US itself, those attacks would alert the continental US defense system, although the overseas installations might obtain only radar warning of the attack. They would probably have been alerted, to some extent, however, by generalized warning derived from general preparations for hostilities.

probably provide no specific advance warning to US intelligence.[13] Moreover, there are two other ways in which the USSR might by 1958 (and possibly somewhat before that year) launch an attack on the US in such a way that no specific warning would be likely before its actual launching:

a. Assuming that the USSR pressed ahead with development of its advance bases in the Chukotski, Kamchatka, and Kola areas, and with the general preparation of its Long-Range Air Force, "normal" flights of aircraft to and from these bases would almost certainly occur in increasing number as the development of the bases progressed. A pattern of activity would tend to be established. Under these circumstances, a considerable number of aircraft—roughly the number engaging in such "normal" activity—would almost certainly be able to take off from these bases (and from those in the Leningrad area) for a surprise attack upon the US without any such unusual prior preparations or assembly as would particularly attract the attention of allied intelligence.

b. Assuming that the USSR acquires an inflight refueling capability (which it can do although there is no evidence at present that the Soviet Long-Range Air Force possesses such a capability) and develops it to the necessary degree, Soviet heavy bombers could also be launched on two-way missions from certain home bases without specific advance warning, and without staging at the advance bases.[14]

VII. Warning from Soviet Preparations to Receive Retaliatory Attacks

46. An important element not included in the foregoing examination is that of Soviet defensive preparations to receive a retaliatory blow from allied power. Minimum preparations would probably include the alerting of air defense forces and the civil defense organization, preparations of military units and installations for air defense, the dispatching of submarines accompanied by increased aerial reconnaissance to locate US carrier forces, and the evacuation of key personnel and possibly segments of population from potential target areas. If steps such as these were not taken, they would constitute serious limitations on the USSR's ability to withstand a retaliatory blow. If they were taken, they would probably provide a warning period of as much as a week to 10 days, and, taken in conjunction with other indicators, would greatly increase the definiteness of any warning US intelligence might be able to give. The risk which the USSR would be willing to accept as a result of neglecting some or all of this type of defensive preparation would depend in part on the degree of success which the Soviet leaders expected their own initial attack to achieve. We believe that in elementary prudence they would be unwilling to forego preparation to receive a retaliatory blow; therefore, some important indicators of this type would probably be obtained.

[13] For full discussion of Soviet long-range capabilities, see NIE 11-7-55.

[14] Only the BEAR (Turbo-prop), with its tentatively estimated characteristics, could reach all targets in the US. See NIE 11-7-55.

NIE 11-4-60 MAIN TRENDS IN SOVIET CAPABILITIES AND POLICIES, 1960–1965

THE PROBLEM

To review significant developments affecting the USSR's internal political situation, economic, scientific, and military programs, relations with other Bloc states, and foreign policy, and to estimate probable Soviet policies and actions over about the next five years.

SUMMARY OF THE ESTIMATE

1. The attempt to forecast developments within the USSR and in Soviet power and policy for five years ahead is subject to some very severe limitations. Our estimative reach in many of the detailed matters discussed in the body of this Estimate is frankly acknowledged to fall well short of such a period. In respect of matters where we have actually made five-year estimates the degree of certainty falls off markedly for the later years. In the summary paragraphs which follow we are dealing with the broader trends which will determine the nature and magnitude of the challenge which the USSR will present to US security in the years ahead. These we believe are predictable in the main, although their particular manifestations clearly depend upon unknown and imponderable factors, or even upon purely fortuitous developments.

The Present Soviet Outlook

2. One of the principal factors which will shape future developments is the outlook of the Soviet leaders themselves. There are two essential aspects of this. One is the Soviet leaders' belief, derived from the Marxist-Leninist ideology which continues to dominate their thinking, that their society and the non-Communist world are locked in an irreconcilable struggle which must continue until their system comes to dominate the world. There is no evidence at present to indicate that the Soviets will come to accept a world system which assumes the genuine coexistence of states and ideologies. For so brief a period as five years, Soviet behavior and policy will surely be marked by fundamental hostility toward the West, and especially toward the US as the principal obstacle to the fulfillment of Soviet aims.

3. A second essential feature of the Soviet outlook in the current period is its high confidence in the growth of the USSR's power and influence. Looking back to the weak and perilous position in which the new Communist regime found itself in 1917, remembering all the internal and external trials it has survived, and considering its growth in relative economic and military power over the last 20 years, the Soviet leaders are encouraged in their doctrinaire expectations about communism's inevitable triumph. That it was a Communist rocket which first ventured into space symbolizes for them that they are marching in the vanguard of history. They think they see a response to their doctrines and influence in the revolutionary turmoils of Asia, Africa, and Latin America. They expect to associate the peoples emerging from colonialism and backwardness with their own cause, mobilizing them against an ever more constricted world position of the Western states. The relative internal stability of the latter at present they see as only a transient phase.

4. While hostility toward the West and confidence in the eventual outcome of the world struggle will inspire Soviet behavior in the period ahead, we do not believe that the result will be policies of recklessness. The Soviet leaders recognize that Western resources remain great, and that the struggle for Communist power in the uncommitted world will be prolonged. They are particularly conscious of the hazards of nuclear war. Moreover, they have numerous problems of their own within the Communist Bloc which may move them to caution. Their policies will be marked by a persistent activism and opportunism, but also by what they consider to be a due measure of caution. More important, however, than the Soviet outlook and aims, especially since these offer little hope for accommodation and genuine peace, are the strengths and resources which the Soviets will be able to bring to the pursuit of their aims.

THE SOVIET POWER BASE

ECONOMIC ASPECT

5. Perhaps the most firmly based of our estimates are those which relate to the growth of Soviet economic power. The Soviet economy has the resources and plant as well as the planning and directing mechanisms to insure steady fulfillment of most of the goals in industrial expansion which the leadership sets. The industrial targets of the Seven-Year Plan (1959–1965), providing for 8.6 percent annual increase in industrial output, will almost certainly be met ahead of schedule. We estimate that by 1965 total investment will reach about one-third of gross national product (GNP), as compared with the present US rate of about one-fifth of GNP. Only in agriculture, which is burdened by a heritage of errors and neglect, will the regime fall well short of its goals, but even here we estimate that output will increase by about 3 to 4 percent per year. The GNP of the USSR in 1959 was somewhat less than half that of the US; it is growing about twice as fast and by 1965 will probably be somewhat more than half of US GNP.

6. GNP is a rough measurement, however. More important in terms of world power competition are the uses to which economic resources are put. The USSR maintains a defense effort judged to be of about the same magnitude as that of the US. The dollar value of Soviet investment in industry in 1959 exceeded the highest US figure, achieved in 1957. For purposes related to national power—defense, science, foreign economic and political operations—the Soviets are increasingly in a position to assign resources freely and without agonizing self-denials. That they are able to provide the resources for national power on a scale equivalent to the US is due to the virtually absolute command which the leadership has over the disposal of resources. It will continue to give the highest priority to purposes related to national power in order to "overtake and surpass" the US. The Soviet regime has bought economic growth and military strength at the expense of the living standards of the Soviet people. But its resources are now great enough so that it feels able to provide for improved living standards also. The consumption level remains low but we estimate that per capita increases will occur over the next five years at the respectable rate of four percent annually. The Soviet challenge in the economic field will be increasingly formidable, not because the USSR has any chance of overtaking the US standard or style of living, but becomes Soviet resources for the competition in power are already great and will continue to grow rapidly.

MILITARY ASPECT

7. As indicated, military power has one of the first claims upon Soviet resources. Our estimates on the development of Soviet military power until 1965 are far less certain than those on the Soviet economy. This is partly due to unpredictable developments during a period of rapid change in military technology. It is due more to gaps in certain kinds of critical information about Soviet military programs. Although in recent years the Soviets have released fuller economic data than previously, on essential matters in the military field they continue to maintain a policy of extreme secrecy, which they evidently view as a major military asset in itself.

8. The most significant development in the military field during the period of this estimate will be the USSR's emergence from strategic inequality, primarily through the buildup of an ICBM force, and also through development of its defense systems against nuclear attack. The overcoming of an inferiority under which the Soviets have operated throughout the postwar period is already having a profound effect on Soviet attitudes and policy. It inspires the confidence remarked upon above, has emboldened the Soviets to challenge the West on a vital issue like Berlin, and has led them to engage the West in other areas around the world formerly conceded to be beyond the reach of Soviet power.

9. The Soviet leaders will not be content with the gains in military power they have made. They will seek, by intensive research and development through the years ahead, as well as by equipping their forces with advanced weapons as these become available, to acquire an advantage over the West. If they succeed, they will press their advantage ruthlessly, though still within what they would consider to be the limits of tolerable risk to their own rule and system. It seems quite clear that in their present view both sides are deterred from the deliberate initiation of general war as a rational course of action. Moreover, with the weapons systems now on hand or likely to be available during the next few years, the Soviets probably do not count on acquiring an advantage so decisive as to permit them to launch general war under conditions which would not gravely menace their regime. Nevertheless, they are building their nuclear striking power with vigor, and we believe that they will build a substantial missile force. What we can learn of Soviet ideas suggests that their long-range striking capability is thought of primarily in terms of deterrence, and of employment for a heavy blow should the Soviets finally conclude that deterrence had failed, rather than in terms of the deliberate initiation of general war.[1] The Soviet missile force will also constitute an important means of political pressure, even though it is never used in actual combat.

10. In order to deal more effectively with the continuing bomber threat the Soviets are incorporating a large number of surface-to-air missiles into their air defense. They are now also doing large-scale research and development on antimissile systems in the hope of obtaining an advantage in this critical aspect of the future weapons balance. By the period 1963–1966 they will probably begin to deploy such a system, though its effectiveness is

[1] The Assistant Chief of Staff, Intelligence, USAF, believes that the evidence of offensive missile and bomber production and deployment shows a definite intent by the Soviet rulers to achieve a clear military superiority at the earliest practicable date. He feels we are entering a very critical twenty-four month period in which the USSR may well sense it has the advantage. The Soviet leaders may press that advantage and offer the US the choice of war or of backing down on an issue heretofore considered red vital to our national interests.

uncertain. Soviet research and development effort will probably also focus on the new threat presented by Polaris.

11. Partly as a result of the increased security the Soviets feel they have gained from their development of a variety of offensive and defensive missiles, they have announced a major personnel reduction in their forces, from about 3.6 to about 2.5 million men by the end of 1961. Barring a serious deterioration in the international situation, we believe the cut will be substantially carried out. We believe that tactical aviation has already been cut by one-half and naval aviation by two-thirds, the latter primarily through elimination of the fighter arm. However, the main weight of the cut will fall on the very large ground forces. Even with the reduction, the Soviets will still have substantial field ground forces: we estimate nearly 1.5 million men organized in 65 divisions averaging two-thirds strength and some 60 cadre divisions at about one-fourth strength. The submarine force will become even more than it is today the primary component of the Soviet Navy, and will include nuclear and missile-carrying types suitable for strategic attack.

12. In sum, the USSR will continue to develop formidable military strength despite the personnel reduction. The Soviet military posture is designed primarily, we believe, to deter general war but also to fight such a war if necessary.[2] Equally, it is intended to bolster the USSR's power position and thereby to promote its general policies. Soviet capabilities for limited war in areas close to Bloc borders are obviously great, but for conflict in more distant areas they are comparatively slight. We do not believe that the USSR intends as a matter of policy to conduct limited war at remote ranges. However, we do not exclude that, with their current tendency to political involvement in remoter areas, the Soviets may seek to develop a greater capacity for intervening militarily, even if only to establish a military presence, in such areas. A really effective ability to do this would presumably depend heavily upon acquisition of base rights and facilities under friendly political arrangements.

SCIENTIFIC ASPECT

13. The Soviets obviously understand that science has become one of the key fronts in the world struggle, not only because of its relations to military capability but also because it is a major element in great power prestige. The scale of their effort, thanks to the heavy investment they made in training scientists in past years, is probably now roughly on a par with that of the US, at least in some fields of the basic sciences and in critical areas related to weapons technology. Presumably the scope of Soviet scientific activity will broaden as needs in these first priority areas are met. The quality of Soviet scientific work in many fields is now such that achievements conferring great prestige are as likely to occur in the USSR as in any other country.

POLITICAL ASPECTS

14. It is in estimating the political aspect of future developments within the Soviet Bloc that the greatest imponderables intrude. The political system within the USSR itself is stable, and it will almost certainly retain its totalitarian features. The regime will not be openly challenged by the Soviet people, who, even though many of them view it with

[2] The Assistant Chief of Staff, Intelligence, USAF, believes the Soviets seek a clear military superiority. See his footnote to paragraph 9.

apathy and ideological disillusionment, are in general hopeful for improvement in the conditions of their life and patriotically moved by the USSR's achievements and its position of world power. If there is change in the Soviet political system it will come from the higher levels of the party and government. In the relatively small group which constitutes the real governing class there are some signs of a desire for more regular participation in policy making, and for more reliance in policy execution on professional expertise instead of party agitational methods. While Khrushchev has avoided or been obliged to avoid the arbitrariness of Stalin, among those who surround him there are probably some who would like to move still further away from the domination of one man in the system. Given Khrushchev's age and state of health he may not survive as the dominating leader throughout the next five years. His successor at the head of the Soviet Government and party may be more restricted in the personal power he wields, but in any totalitarian system political developments are likely to depend heavily on the qualities and style which individual personalities bring to the exercise of great and arbitrary power.

15. In the area of political developments within the Communist Bloc it is the evolution of relations among the Bloc states which raises the greatest uncertainties at present. In general, the states of Eastern Europe have gained in economic strength and political stability in recent years, despite the continuing alienation and resentment of large parts of their populations. There seems little doubt that, with the more flexible and indirect methods of control the USSR has been employing since 1956–1957, it will be able to maintain a generally effective hegemony. However, China has raised a fundamental challenge to Soviet leadership of the Bloc. Even if some way is found to resolve the issues posed by China's desire to pursue a more militant policy toward the West, it raises the serious question as to whether the long-term unity of the Bloc under Soviet leadership can be maintained. We believe that there is a trend away from monolithic unity, and that in the long run, if China is to remain within the Bloc, a looser relationship is bound to develop. The future course of Sino-Soviet relations will obviously have profound consequences for the nature of the challenge which communism poses for the Free World. The West may be faced either with new dangers or new opportunities, or both.[3]

Soviet Policies Toward the Non-Communist World

16. The general Soviet strategy for carrying on the world struggle in the present phase rests on two propositions. The first is that general nuclear war must be avoided because the costs in physical damage and social disintegration would be intolerable. The second is that the world position and power of the "imperialist" states can be undermined by a persistent and aggressive campaign waged by methods short of war—political struggle, economic and scientific competition, subversion. Political struggle takes the form of a constant agitation designed to capture and organize in broad mass movements the sentiments which focus on the great issues of the current period—peace, disarmament,

[3] The Assistant Chief of Staff for Intelligence, Department of the Army, and the Director for Intelligence, Joint Staff, believe that, in spite of Sino-Soviet frictions, the USSR and Communist China will continue to be firmly allied against the West and will render one another mutual support whenever an important interest of one or the other is threatened by the non-Communist world.

anticolonialism, social justice, economic development. By manipulating these issues and by dramatizing the growth of Soviet power, the Soviets are also trying to align the governments of the underdeveloped and uncommitted states with the Bloc, and against the West. The Soviet leaders hope that the result will be a progressive isolation and loss of influence for the Western powers, divisions among them, and a decline in their ability to deal effectively with threats to their interests. This is what the Soviets mean by "peaceful coexistence"—a strategy to defeat the West without war.

17. This is not a strategy which aims immediately at the revolutionary seizure of power by Communist parties and the setting up of Communist regimes. The Soviets know that there are few countries where the Communists are strong enough to undertake such action, and where they themselves could count upon being able to deter intervention by non-Communist forces. The "peaceful coexistence" strategy is aimed mainly at gradually eliminating Western and building up Soviet influence around the world. The Soviets naturally expect that conditions will thereby be created which are favorable to the growth of Communist movements and which will sooner or later permit the latter to acquire state power peacefully, or by revolutionary action if necessary. Even though overt seizure of power is not now the main aim of the Soviet strategy, over a five-year period situations might arise where the gains from such action would seem important enough to the Soviets so that they would be willing to depart from their present general line.

18. The general line of Soviet policy estimated in the two preceding paragraphs falls within a range which excludes, on the one hand, the deliberate assumption of serious risks of general war, and on the other, abandonment of active struggle against the West. Within these limits we believe that the Soviet leaders will display both militancy and conciliation, at various times and in various proportions as seems to them most profitable. However, the Chinese challenge to Soviet authority involves basic questions of foreign policy, and brings severe pressure to bear on Soviet policy decisions. In trying to adjust to Chinese pressures, the Soviets may go farther in the direction of militancy and risk-taking than they otherwise would. On the other hand, if the Soviets should conclude that the Chinese were pushing them towards unacceptable dangers, they might move as a matter of temporary expediency toward a greater degree of stabilization in their relations with the West than they would otherwise consider, though without altering their long-term aim of establishing Communism throughout the world.[4]

19. As a general rule, we believe that the Soviets would consider that the initiation of limited war with Soviet or even Bloc forces entailed unacceptably high risks and political liabilities. However, it cannot be excluded that situations will appear in which they would conclude that some prize was great enough, and the military and political risks acceptable enough, to justify resort to such action. The Soviets are aware, however, that any limited war carries a danger of expanding into general war. We believe, therefore, that their attitude toward the involvement of Soviet or Bloc forces in local and limited war will be a very cautious one, and will be governed by their estimate of the risks and advantages, both

[4] The Assistant Chief of Staff, Intelligence, USAF, agrees that the Chinese challenge to Soviet authority will, undoubtedly, have its effect on Soviet policy toward the non-Communist world; however, he believes that the relationship of Soviet military power vis-a-vis the US is the essential determinant. Further, as expressed in his footnote to paragraph 9, he believes that should the Soviets feel that they have achieved a clear military superiority, they are likely to adopt policies involving serious risks of general war.

political and military, in each situation. Even so, there is always a possibility that they may miscalculate risks.

20. Negotiations with the Western Powers over outstanding issues are conceived by the Soviets as one of the modes of waging the struggle of "peaceful coexistence." They hope that the pressures which they attempt to build up against the West will result in concessions at the negotiating table. Intervals of more accommodating behavior and appeals for relaxed tensions are intended to encourage the making of such concessions. We expect this alternation of pressure and accommodation to be the regular pattern of Soviet behavior with respect to negotiation in the years ahead. Since the U-2 incident in May 1960 the Soviets have adopted a hostile and aggressive attitude which has made effective negotiation impossible. We believe that within the next six months or so the Soviets are likely to moderate this attitude and to attempt to get negotiations started again. It is also possible, however, that on the Berlin issue, where negotiation has so far failed to get them results, they will resort to intensified pressure and threats in an attempt to force the West into high-level negotiations under more unfavorable conditions.

21. We do not believe that the Soviets have a five-year plan for foreign policy in the sense that they set themselves particular goals to accomplish within a set time. Their policy is marked rather by an extraordinary opportunism, and in recent years by rapidity of response and vigor in execution. Over the next five years they probably look for new developments favorable to their interests to occur in a number of areas, but more especially in Africa, Latin America, Japan, Indonesia, and Iran. They probably intend to give particular attention to establishing a diplomatic and economic presence in Africa, to stimulating and exploiting movements on the Castro model in Latin America, and to encouraging the growth of a radical anti-American mass movement in Japan. Above all, however, they intend to build up their base of power within the Bloc itself, in the belief that during the next several years they can considerably improve their relative power position vis-a-vis the West. They believe that if they do so, more opportunities for Communist expansion, and more readily exploitable ones, will open up for them.

NIE 11-4-63 SOVIET MILITARY CAPABILITIES AND POLICIES, 1962–1967

DISCUSSION

I. Soviet Military Policy

A. BASIC VIEWS ON WAR AND MILITARY POLICY

1. The Soviets see military power as serving two basic purposes: defense of their system and support for its expansion. Thus, one of the most important objectives of Soviet military policy is to deter general war while the USSR prosecutes its foreign policies by means short of actual hostilities involving Soviet forces. Military power is constantly brought into play in direct support of these policies, through the threats which give force to Soviet political demands, through the stress on growing power which is intended to gain respect for the Soviet state and its Communist system, and through the military aid and support rendered to allies, friendly but neutral regimes, and anti-Western movements.

2. The Soviet leaders realize that their deterrent must be credible in the sense that it rests upon powerful military forces. Moreover, they recognize that deterrence may fail in some key confrontation in which, despite their best efforts to retain control over risks, either they or their opponents come to feel that vital interests are under challenge. Against this contingency they wish to have a combination of offensive and defensive capabilities which will enable them to seize the initiative if possible, to survive enemy nuclear attack, and to go on to prosecute the war.

3. The Soviets evidently believe that the present overall military relationship, in which each side can exert a strong deterrent upon the other, will probably continue for some time to come. The Soviets are vigorously pursuing programs of research and development in advanced weapons, hoping if possible to create a strategic balance favorable to them. It is possible that some future technological breakthrough or advance would persuade them that they had acquired a decisive advantage which permitted them to take a different view of the risks of general war. We do not believe, however, that the Soviets base their military planning or their general policy upon the expectation that they will be able to achieve, within the foreseeable future, a military posture which would make rational the deliberate initiation of general war or conscious acceptance of grave risks of such a war.

4. A number of Soviet statements in recent years have expressed the view that limited war involving the major nuclear powers would inevitably escalate into general war. While such statements are intended in part to deter the West from local use of force, this official view also reflects a genuine Soviet fear of the consequences of becoming directly engaged in limited war involving Soviet and US forces. This probably also extends to involvement of Soviet forces with certain Allied forces in highly critical areas, notably Western forces in the European area. Nevertheless, they might employ their own forces to achieve local gains in some area adjacent to Bloc territory if they judged that the West, either because it was deterred by Soviet nuclear power or for some other reason, would not make an effective military response. They would probably employ Soviet forces as necessary if some Western military action on the periphery of the Bloc threatened the integrity of the Bloc itself. Should the USSR become directly involved in a limited war with US or Allied forces, we believe that the Soviets would not necessarily expand it immediately into general war, but that they would probably employ only that force which

they thought necessary to achieve their local objectives. They would also seek to prevent escalation by political means.

5. Recent Soviet military writings call for professional study of the problems of nonnuclear combat, which could lead to some modification of the official view on limited war. However, we believe that the attention now being devoted to this problem is primarily responsive to indications of US interest in building NATO's capabilities for nonnuclear combat. In our view, it does not reflect any new Soviet conclusion that the USSR can now launch such wars without great dangers of subsequent escalation.

6. The USSR has regularly recognized the importance of the "war of national liberation," in which pro-Soviet or anti-Western forces challenge colonial or pro-Western regimes in a primarily internal conflict. In practice, Soviet behavior has followed neither the course of full support to all these wars, as Soviet propaganda often alleges, nor the course alleged by Khrushchev's Chinese critics, who claim that he withholds support entirely because of exaggerated fears that such a conflict might spark a general war. The USSR has rendered active assistance in some cases, such as Laos and Yemen, and little or none in others, such as Algeria and Angola, depending upon such practical factors as accessibility, the risk of defeat, and the attitude of other powers involved.

7. The USSR has also shown a recent willingness to provide some non-Bloc recipients of its military aid with more advanced equipment than heretofore. In some cases, notably Cuba and Indonesia, Soviet personnel have been employed to man this equipment, and are training indigenous specialists to operate it. This represents a significant departure from previous Soviet practice, which may be extended to other areas in the future.

8. As new and favorable opportunities arise, the Soviets will continue to offer these various kinds of assistance, and they may do this more frequently and aggressively in the future if their efforts to expand Soviet influence by political and economic means encounter continued frustration. We believe, however, that the Soviets will remain chary of any great commitment of prestige to the support of belligerents over whom they do not exercise substantial control or in circumstances in which they feel that winning is unlikely, and they will seek to avoid risk of widened hostilities which might result from "wars of national liberation." In particular, we believe that the Soviets will be very reluctant to commit their own forces openly in conflicts where they would risk a direct confrontation with US forces.

B. SOVIET MILITARY POLICYMAKING

9. The application of these basic attitudes to particular situations and to the allocation of resources does, of course, pose serious policy problems. A number of additional factors have long affected the character of Soviet military policy. Geography and the traditions bound up with historical experience have inclined the Soviets toward a military preoccupation with Western Europe and a stress on large-scale ground combat. The capabilities and structure of US and other opposing forces influence directly both the size and shape of Soviet forces and exert a general upward pressure upon requirements in all fields. Perhaps most important is the technological and economic base of the nation, which constantly offers prospects for more effective weapons but also determines the extent to which these opportunities can be exploited without too great a sacrifice in other programs.

10. These factors, pointing in many contradictory directions, do not make for easy or unanimous decisions. Indeed, we have clear evidence of disagreement, compromise, and

even reversal in the formulation of military policy in the last three years. This process of policymaking in the USSR appears in large part to involve the same problems familiar to US decision-makers. In addition, however, certain special features stand out. Fully informed Soviet military discussion, for example, seems to involve a smaller circle than in the US. Beyond the political leadership, some military officers, and a limited number of scientists and engineers, we know of no body of civilian advisers or publicists in the USSR comparable to the social scientists involved in the evolution of US military thinking. This is in part due to the great Soviet emphasis on security, which has the additional effect of reducing the flow of information within the officer corps. As a result, the Soviet military appear to experience special difficulty in adjusting their doctrine and concepts to the rapid changes characteristic of the postwar period. The continuing major influence of World War II commanders and the vivid memories of the Soviet experience in that war also contribute to a resistance to new concepts which is evident in professional discourse.

11. Military programs have become more complex and expensive, and the professional recommendations of the military leadership on military problems have a greater impact on economic and foreign policy decisions. Furthermore, the political climate which has developed under Khrushchev is one which permits continuing discussion on a variety of problems, and the military leaders have used this opportunity to expound their views. With military and economic debates proceeding simultaneously and in close dependence on each other, it seems likely that the arguments of the marshals have been supported by those political leaders who did not wish to permit programs for consumer goods to impinge upon allocations to heavy industry.

12. We do not believe that the military aspires to an independent political role within the political system, and if it were to, party traditions and controls appear strong enough to defeat any efforts in this direction. But if, as we expect, the military and economic choices facing the USSR become more acute, the senior officers will probably find themselves more deeply involved in matters of general policy.

C. THE RECENT COURSE OF MILITARY POLICY

13. The most important viewpoints in the controversy over military policy of the last few years have been those represented by Khrushchev and a few military theorists, on the one hand, and the majority of the senior military leaders, on the other. Three major differences have distinguished Khrushchev's approach to defense policy from that of the military leaders. First, Khrushchev is heavily concerned with the political uses of military power, whereas the professional responsibilities of the marshals require them to look in the first instance to actual war-fighting capabilities. Second, Khrushchev has asserted that a general war is almost certain to be short, with victory decided in the strategic nuclear exchange and with conventional arms, particularly theater forces, playing a quite secondary role. Most military leaders, on the other hand, appear to believe that general war would probably, but not certainly, be short but that, in any event, its conduct would require high force levels for most of the traditional service arms, including a multimillion man army. Third, Khrushchev is far more concerned than the marshals to keep military expenditures in check in order to meet what he regards as pressing needs in the civilian economy.

14. All these considerations were involved in the reorganization of the armed forces which Khrushchev inaugurated in January 1960. The essence of his plan was to place main

reliance on nuclear missile forces and, on this basis, to reduce military manpower substantially and to accelerate the retirement of older weapons. This, he asserted, was the force structure best suited both to deter war and to fight one if necessary; moreover, it would release men and money for the civilian economy.

15. From Khrushchev himself we know that this plan and its strategic justification were accepted only reluctantly by the military leadership. A controversial discussion ensued, encouraged by the regime, in which high officers debated, polemicized, and explored the military implications of modern warfare in a far more systematic fashion than previously. Several schools of thought became apparent, but a predominant view soon emerged which accepted the likelihood that the initial phase of a general war would be decisive, but went on to argue that even a relatively short war would require large forces of all types capable of defeating comparable enemy forces, overrunning base areas, and occupying territory in Eurasia. This discussion also focused attention on the enormous difficulties of mounting major military operations after receiving the full weight of a Western first strike, and the resulting importance, if in the Soviet view war became imminent and unavoidable, of seizing the strategic initiative by a pre-emptive attack.

16. At present, official military doctrine holds that a general war will inevitably involve the massive use of nuclear weapons, will begin with a strategic exchange, and will develop almost simultaneously along fronts of engagement as well. Strategic missile forces will play the primary role. The course and outcome of the war may well be decided in its initial phase by strategic nuclear weapons. However, the Soviets hold that such a conflict will not necessarily be short, and envisage the possibility of a long war involving protracted operations in Eurasia. Therefore, while current doctrine emphasizes a military policy of building strategic attack and defense capabilities, it supports as well the maintenance of large theater and naval forces, for use both in the initial and the possible subsequent phases of a general war.

17. We believe that debate continues in the USSR, not only over subsidiary propositions, but perhaps over some of the central tenets of this doctrine. The course of the debate was heavily influenced by external events in 1960–1961 which, intruding upon the discussion, undermined some of Khrushchev's contentions and permitted the military to retrieve some concepts which he had discarded. Thus the U-2 affair cast doubt on the adequacy of Soviet air defenses, on the efficacy of Soviet security, and on the wisdom of Khrushchev's efforts to relax tensions in relations with the US. In the following year, the US took decisions to step up both its strategic attack and general purpose forces. In Vienna, Khrushchev determined that the US did not regard the relationship of military power as requiring it to make major concessions on the Berlin question. All these developments called into question the adequacy of the Soviet military posture, both for supporting foreign policy and for conducting general war if necessary. In these circumstances, Khrushchev made such demonstrative military moves as the public suspension of the manpower reductions and the resumption of nuclear tests.

18. At about the same time, another burden was laid on Soviet military policy-making. For some months, US public disclosures had hinted that Soviet ICBM strength might be much smaller than had previously been believed. Beginning in the fall of 1961, the US began to assert this conclusion with great conviction, and to assert more strongly that the US was the strategic superior of the Soviet Union. From US statements and behavior, the Soviets could almost certainly judge that their security had been penetrated in an important way, probably one which, by permitting the US to locate Soviet targets,

had a tangible effect upon the military balance. Their fears that no major Western concessions on Berlin would be forthcoming must have been strengthened. And the image of Soviet superiority, which they had heavily exploited to document their claims of the inevitable triumph of their system, was badly damaged.

19. It was against this background that the USSR took its decision to deploy strategic missiles to Cuba. This move involved a host of policy considerations and judgments which are not yet fully clear. In its military terms, however, it appears to have been a response to the question of how to create new opportunities for Soviet foreign policy by improving the strategic position of the USSR vis-a-vis the US, at some acceptable cost and at some early date. Even deployment at the levels detected promised a significant increase in first-strike capabilities for general nuclear war, and the Soviets may have intended to follow this up by establishing a larger missile force as well as a submarine base.

20. Khrushchev, however, probably considered its main impact to be psychological. At one level, the deployment and its acceptance by the US was intended to demonstrate Soviet might and US inability to contain it, thereby reversing the tendency of world opinion to regard the West as strategically superior. At another, however, it was intended to increase the deterrence laid upon the US in cold war confrontations. Khrushchev evidently felt that, despite all the military problems involved in making effective strategic use of Cuba in wartime, the deployment would have a powerful impact on US opinion which would reduce resistance to his political demands, in the first instance those concerning Berlin.

D. PROBLEMS OF FUTURE MILITARY POLICY

21. The Cuban adventure and its outcome both highlighted and heightened the dilemma of the Soviet leaders. Both the deployment and its reversal constituted a tacit public admission that the USSR was in a position of strategic inferiority. Among its other results, the Cuban fiasco has almost certainly thrown the Soviets back onto a further re-evaluation of their strategic posture.

22. Programs already under way will largely govern the size and composition of Soviet strategic forces through about mid-1964, but new decisions taken this year could significantly affect force levels thereafter. We are unlikely to learn directly of such decisions. Moreover, the physical activities which might reveal their nature will probably not be apparent for another year or more. In considering future Soviet force levels, it is therefore necessary to explore the various alternatives now open to the USSR.

23. Confronted with the continuing buildup of US forces for intercontinental attack programmed for the next few years, Soviet planners may be considering a wide range of alternatives. At one extreme would be an attempt to achieve such a clear superiority over the US in strategic offensive weapons that they would have a high assurance of destroying US nuclear striking forces prior to launch. At the other extreme would be the acceptance of continued strategic inferiority, perhaps coupled with genuine efforts to reach agreement with the West on arms control.

24. The first of these extreme alternatives is probably now regarded as unattainable. Thousands of Soviet missiles would be required to give the Soviet leaders a high assurance of destroying even the fixed bases of US nuclear forces programmed for the mid-1960's. We do not believe that the Soviet leaders would be prepared to impose a strain of this magnitude upon the Soviet economy. In addition, the Soviets would almost certainly

expect the US to detect such an effort, and thereupon to step up its own program so as to raise Soviet requirements still higher. Moreover, US warning capabilities, fast reaction times, and mobile forces (airborne bombers and missile submarines) already have reduced Soviet capabilities, against US retaliatory forces. We believe that the Soviets will continue to estimate that, throughout the period of this estimate, the US will retain retaliatory capabilities which could not be eliminated by such striking forces as the USSR could acquire.

25. The second of these extreme alternatives might be considered by the Soviet leaders. Even if current strategic weapons programs were allowed to level off after 1964, the Soviets would possess a powerful deterrent force. Moreover, they might hope to reduce US superiority by means of disarmament agreements. But the main appeal of this alternative would be economic; resources would in time be made available to reverse the current slowdown in economic growth. However, we have seen as yet no persuasive indications that the USSR is prepared to move very far in this direction. The Cuban venture has indicated that, at least to date, the Soviet leaders are far from willing to accept a position of strategic inferiority.

26. Between these extreme alternatives, we believe that the Soviets have almost certainly considered an effort to attain rough parity with the US in intercontinental weapon systems. Soviet military leaders almost certainly have urged enlarged and improved forces of ICBMs and missile submarines. However, a major Soviet effort to attain parity in the near term would require either a substantial increase in the Soviet military budget or sharp cuts in other types of forces. Moreover, the Soviets would almost certainly reason that the US would detect an effort of such magnitude, and that they could have no assurance of winning the intensified race which would ensue. Our evidence does not indicate that the Soviets are attempting to match the US in numbers of weapons for intercontinental attack; we believe, however, that they will attempt to offset US superiority by other means.

27. Soviet statements and military writings suggest that the Soviet leaders see in technological achievements the means by which they may improve their total strategic position relative to that of the US. This consideration may lie behind the testing of very high-yield weapons, the claimed development of a global missile, the high priority given to the antimissile program, and the Soviet interest in military space programs. By such means, the Soviets may attempt to attain rough parity or even superiority in the total strategic context, although they remain numerically inferior in delivery vehicles. Hardened ICBMs and submerged-launch submarine missiles will contribute to Soviet strategic capabilities. In addition, over the next few years the ICBM force will probably come to include new large missiles, armed with very high-yield warheads or capable of global ranges. Moreover, the USSR is almost certainly investigating the feasibility of space systems for military support and offensive and defensive weapons.

28. In defense against strategic attack, the major new element is the antimissile program, where deployment of one system has already begun at one location, and research and development toward a more advanced capability is continuing. The Soviets may see a possible solution to their strategic confrontation with the US in a combination of antimissile defense plus very effective though numerically inferior intercontinental striking forces. The technical difficulties as well as the great expense of any extensive antimissile deployment will be restraining influences. Nevertheless, we believe that deployment of antimissile defenses may be the largest new Soviet military program in the period of this estimate.

29. Although we believe that Soviet military policy is most likely to continue along current lines, we cannot exclude the possibility of new departures in military policy, perhaps resulting in major changes in the composition of the Soviet military establishment and in the relative emphasis given to forces designed to accomplish the major military missions. Drastic cuts in the theater field forces remain a possibility; while Khrushchev's proposals for manpower reductions have been shelved for the present, economic pressures and developments in military technology almost certainly will cause this subject to be reconsidered. It is also possible that the increasing involvement of the USSR in the more remote areas of the world will lead to the development of new capabilities for distant, limited military action. In this connection, the Soviets may attempt to acquire base and logistical support rights in key non-Bloc countries, but we have no evidence that the USSR has raised this question with these countries.[1]

30. In general, Soviet military policy will continue to be shaped, not only by a variety of strategic, historical, technical, economic and political factors, but also by differing views about the relative importance of these factors, and shifting compromises among these views. As a result, we believe that the numerous aspects of this policy will not always be wholly consistent with each other, and that force structure and future programming will reflect neither a fully-integrated strategic doctrine nor a firm timetable for achieving specified force levels. In any case, we do not believe that the Soviets conceive of existing weapons systems as the answer to their military problem or that they have fixed and inflexible plans for their force structure in the period five to 10 years from now. They have debated and revised some of their ideas, and they will probably do so again. They have made scientific military research and the development of new weapons matters of high urgency, and they have a demonstrated capability to concentrate human and material resources on priority objectives. If they develop new concepts or new weapons which give promise of military and political advantage, they will seek to add them rapidly to their arsenal and to gain maximum benefit from them. Thus, during the next five years, we expect the Soviets to be working on even more advanced weapons with which they may hope to enhance their capabilities at a later date.[2]

II. Soviet High Command Structure

31. We believe that during the past two or three years the Soviet military high command structure has been modified to speed the process of initiating or responding to strategic nuclear attack. The growth of nuclear and missile forces on both sides has almost certainly persuaded the Soviets to establish the command and control channels necessary for the swift initiation of military operations upon the decision of the political leadership.

32. We have information, some of it from classified documents and some from public statements, about both a Supreme Military Council and a Supreme High Command. Khrushchev is chairman of the Council and Supreme High Commander. The Council, a body of high-level party, government, and military officials, has existed since before

[1] For a discussion of the limitations imposed on such Soviet overtures by the receptivity of other countries, see NIE 10-63, "Bloc Economic and Military Assistance Programs," dated 10 January 1963.

[2] With reference to paragraphs 23–30, see the Assistant Chief of Staff, Intelligence, USAF, footnote to Conclusion E.

World War II to provide a forum for discussion and decision on major issues of military policy. The Supreme High Command directed military operations during World War II with Stalin at its head, but was disbanded thereafter. Such information as we have suggests that steps have been taken in recent years to designate membership in the Supreme High Command and to develop procedures to permit the quick assumption by this body of top level control of military operations under Khrushchev should events so dictate.

33. Adjustments in the structure of the Soviet high command have apparently been closely related to the growth of the USSR's strategic defense and long-range missile forces. A new rocket command was established in 1960 and designated a main component of the Soviet armed forces. This change followed by about five years the elevation of the Soviet air defense component to similar status. At present, there are five major force components administered by main directorates or equivalent headquarters within the Ministry of Defense: ground, naval, air, air defense, and rocket.

34. Highly centralized civilian control over the Soviet military establishment is exercised through the Council of Ministers, which includes the Minister of Defense. The Minister is assisted by the unified General Staff of the armed forces, which formulates the overall military program and would probably constitute the principal headquarters element of the Supreme High Command in time of war. Party and government leaders reportedly participate regularly in the deliberations of the Supreme Military Council. Additional channels for exercising party control over the military include the Main Political Directorate of the armed forces and the numerous party officials who are assigned to all levels of the military establishment.

35. The flow of operational orders from the Minister of Defense to the Soviet armed forces follows no rigid or consistent pattern. Commanders in Chief of the Strategic Rocket Forces, Long Range Aviation, the Air Defense Forces, and the Navy are believed to have direct operational control over the forces assigned to them. On the other hand, ground force components are operationally controlled by the commanders of the Military Districts and the Groups of Forces. The Commander in Chief of the Air Force similarly has no direct operational control over air components. The operations of other than Long Range Aviation air elements are controlled by the commands or forces to which they are assigned, i.e., commanders of Groups of Forces, Military Districts, Air Defense Districts, Fleets, and Airborne Forces.

NIE 11-4-64 MAIN TRENDS IN SOVIET MILITARY POLICY

West remained unfavorable. The economic strain of the arms competition loomed as costly as ever. There is evidence of considerable hesitation and re-evaluation in Soviet policy since the failure of the Cuban missile venture, although since about mid-1963, a number of developments have occurred which suggest the general direction Khrushchev proposes to follow. In the economic sphere, short-term plans for 1964–1965 have been revised in order to shift resources, notably to the chemical industry. Consistent with this has been a change in foreign policy tactics, beginning with the test ban, in an effort to relax East-West tensions. The attempt to create a more favorable international climate, in turn, has allowed Khrushchev to secure reductions in the overt defense budget as well as to propose some reductions in military manpower. The sum total of these various steps in related fields suggests that Khrushchev has settled on a general line of policy to contain the arms race, if only in a limited way, and to reduce some of its burden on the Soviet economy.

19. In strategic terms, this line of policy suggests a recognition of the necessity to accept the general balance of power which emerged in the Cuban crisis. Presently, and for some time to come, the Soviet strategic forces will be numerically inferior to those of the US and more vulnerable to attack. The Soviet leaders must recognize, therefore, that the US would enjoy a considerable advantage should it strike first, and that the relative invulnerability, the fast reaction time, and the mobility of US strategic power make a Soviet first strike completely irrational. Nevertheless, in assessing the military balance, the Soviets are confident that they possess a credible deterrent based on both their massive capabilities to devastate Eurasia and their growing intercontinental striking power. Thus, the Soviets see the present situation as one in which both sides are deterred from deliberately initiating general war or from knowingly initiating courses of action which would involve grave risk of such a war.

II. Factors Affecting Future Soviet Military Policy

20. Soviet decisions as to force structure and military programs over the next several years are likely to be made in the context of a situation in which, although the US enjoys a clear strategic advantage, a condition of rough mutual deterrence exists. The Soviets will seek to improve their strategic capabilities *vis-a-vis* the US, however, policy decisions will be influenced by the continuing strain on economic resources, and the pressure arising from competition with the US in scientific and technological developments with military applications. Such decisions will be greatly influenced also by the Soviet estimate of the political situation, the opportunities which it affords, and the contribution which military power can make to the realization of these opportunities.

SPECIAL NATIONAL INTELLIGENCE ESTIMATE NUMBER 85-3-62 THE MILITARY BUILDUP IN CUBA 19 SEPTEMBER 1962

THE PROBLEM

To assess the strategic and political significance of the recent military buildup in Cuba and of the possible future development of additional military capabilities there.

CONCLUSIONS

A. We believe that the USSR values its position in Cuba primarily for the political advantages to be derived from it, and consequently that the main purpose of the present military buildup in Cuba is to strengthen the Communist regime there against what the Cubans and the Soviets conceive to be a danger that the US may attempt by one means or another to overthrow it. The Soviets evidently hope to deter any such attempt by enhancing Castro's defensive capabilities and by threatening Soviet military retaliation. At the same time, they evidently recognize that the development of an offensive military base in Cuba might provoke US military intervention and thus defeat their present purpose. *(Paras. 1–11)*

B. In terms of military significance, the current Soviet deliveries are substantially improving air defense and coastal defense capabilities in Cuba. Their political significance is that, in conjunction with the Soviet statement of 11 September, they are likely to be regarded as ensuring the continuation of the Castro regime in power, with consequent discouragement to the opposition at home and in exile. The threat inherent in these developments is that, to the extent that the Castro regime thereby gains a sense of security at home, it will be emboldened to become more aggressive in fomenting revolutionary activity in Latin America. *(Paras. 18–21)*

C. As the buildup continues, the USSR may be tempted to establish in Cuba other weapons represented to be defensive in purpose, but of a more "offensive" character: e.g., light bombers, submarines, and additional types of short-range surface-to-surface missiles (SSMs). A decision to provide such weapons will continue to depend heavily on the Soviet estimate as to whether they could be introduced without provoking a US military reaction. *(Paras. 22–28)*

D. The USSR could derive considerable military advantage from the establishment of Soviet medium and intermediate range ballistic missiles in Cuba, or from the establishment of a Soviet submarine base there. As between these two, the establishment of a submarine base would be the more likely. Either development, however, would be incompatible with Soviet practice to date and with Soviet policy as we presently estimate it. *It would indicate a far greater willingness to increase the level of risk in US-Soviet relations than the USSR has displayed thus far, and consequently would have important policy implications with respect to other areas and other problems in East-West relations. (Paras. 29–33)*

E. The Latin American reaction will be to the evidence of an increased Soviet commitment to Cuba, rather than to the technical implications of the military buildup. Many Latin Americans will fear and resent a Soviet military intrusion into the Hemisphere, but will regard the problem as one to be met by the US and not their responsibility.

We estimate the chances are better now than they were at Punta del Este to obtain the necessary two-thirds OAS majority for sanctions and other steps short of direct military action aimed at Cuba. If it became clear that the USSR was establishing an "offensive" base in Cuba, most Latin American governments would expect the US to eliminate it, by whatever means were necessary, but many of them would still seek to avoid direct involvement. *(Paras. 34–37)*

SPECIAL NATIONAL INTELLIGENCE ESTIMATE
53-2-64
1 OCTOBER 1964
THE SITUATION IN SOUTH VIETNAM

NOTE: This is an estimate as approved by the United States Intelligence Board. No further distribution will be made.

Submitted by the
DIRECTOR OF CENTRAL INTELLIGENCE

Concurred in by the
UNITED STATES INTELLIGENCE BOARD

As indicated overleaf
1 October 1964

CENTRAL INTELLIGENCE AGENCY

1 October 1964

SUBJECT: SNIE 53-2-64: THE SITUATION IN SOUTH VIETNAM

THE PROBLEM

To examine the situation as it has developed since early September, and to assess its implications for the US.

CONCLUSIONS

A. Since our estimate of 8 September 1964* the situation in South Vietnam has continued to deteriorate. A coup by disgruntled South Vietnam military figures could occur at anytime. In any case, we believe that the conditions favor a further decay of GVN will and effectiveness. The likely pattern of this decay will be increasing defeatism, paralysis of leadership, friction with Americans, exploration of possible lines of political accommodation with the other side, and a general petering out of the war effort. It is possible that the civilian government promised for the end of October could improve GVN esprit and effectiveness, but on the basis of present indications, this is unlikely.

B. We do not believe that the Viet Cong will make any early effort to seize power by force of arms; indeed, we doubt that they have the capability for such a takeover. They will continue to exploit and encourage the trend toward anarchy, looking for the emergence of a neutralist coalition government which they can dominate.

---

* SNIE 53-64, "Chances for a Stable Government in South Vietnam," dated 8 September 1964.

DISCUSSION

THE GVN

1. *Continued Political Deterioration.* Political conditions in South Vietnam have continued to deteriorate since our estimate of early September.† Despite efforts by Prime Minister Nguyen Khanh to stabilize the situation, he has been faced with an attempted coup, rioting and demonstrations in the northern provinces, a massive labor strike in Saigon, and an armed revolt by Montagnard elements among the Special Forces. Khanh's authority, already weakened by the Buddhist-student crisis in August, has been further diminished, and the degree of his support within the military establishment is increasingly in question. Most of the non-Communist power elements appear to be marking time, pending their assessment of the civilian government which Khanh has promised will be formed by the end of October.

2. *The Picture in Saigon.* South Vietnam is almost leaderless at the present time. General Khanh has retained his position by making concessions to various interest groups—political, religious, students, military, and labor—which have pressed their demands upon him. In turn, these groups still seem bent on pursuing self interest and factional quarrels almost to the point of anarchy. A lack of sense of purpose and an absence of direction from above have seriously affected morale and created passiveness and apathy within the civil law enforcement agencies. Government ministries in. Saigon are close to a standstill, with only the most routine operations going on. Cabinet ministers, as well as second-level bureaucrats, freely express their pessimism, and even though US and GVN officials are again meeting on pacification and other joint planning, these meetings are not being followed by action from the Vietnamese side.

3. *GVN Military Morale and Effectiveness.* The continuing disarray of the Saigon government, power struggles within the military leadership, and the activities of self-seeking politicians and religious leaders have adversely affected morale within the military establishment. However, the existing level of effectiveness of combat operations does not seem to have been seriously affected as yet. Nevertheless, continuing political instability would almost certainly aggravate such longstanding deficiencies in the Vietnamese military effort as inadequate motivation, initiative, and aggressiveness. A continuing lack of firm direction, and further squabbling among senior officers in particular, could depress the morale of the troops and junior officers to the critical point. Although the GVN armed forces have long had a high rate of desertion by individuals, there have been no important unit desertions or defections. If military morale continues to decline, however, desertion and defections within both the military and paramilitary services may occur on a larger scale, perhaps even by organized units.

4. *Signs of Defeatism in GVN Leadership.* High-ranking ARVN officers have confessed to US officers deep discouragement at the lack of leadership and direction. The J-3 of the Joint General Staff has indicated that he feels little reason even to discuss further pacification planning; various high-ranking field commanders have expressed similar pessimism; and General Khanh himself has shown signs of being overwhelmed by his responsibilities.

5. *The Situation in the Countryside.* The near paralysis of government initiative in Saigon appears to be spreading rapidly to outlying areas. Although the southern areas still

†SNIE 53-64 "Chances for a Stable Government in South Vietnam," dated 8 September 1964.

appear relatively unaffected by the crises of the past several weeks, governmental authority has declined seriously in the northern coastal provinces where provincial and police officials are apparently receiving little guidance from Saigon. In such urban centers as Hue, Danang, Qui Nhon, and Nha Trang, Vietnamese commanders have repeatedly failed to intervene in civil disturbances and rioting on the grounds they lacked precise orders; in some instances, actual authority has passed by default to extremist "vigilante" groups, such as the "People's Salvation (or Revolutionary) Council" (PRC). The nature of the provincial bureaucracy is such that it can rock along for considerable time, carrying out existing programs despite political deterioration in Saigon. Nevertheless, continued confusion and inaction in Saigon, or another coup, could rapidly produce a critical deterioration in government in the countryside. A slippage in morale and in programs among provincial administrations, at least in the central provinces, has already begun.

6. *The Peoples Revolutionary Council (PRC).* The PRC has established local councils in many coastal cities and may seek to form a chapter in Saigon, where two PRC leaders have recently been named to the new 17-men High National Council. The aims of the PRC are not clear, but the local councils seem vulnerable to Viet Cong penetration, and the fact that they have assumed government powers in some provincial cities tends to undermine Saigon's control and to damage the morale of civil servants.

7. *The Montagnard Problem.* The Rhade revolt of 20 September and the continuing possibility of further and more general uprisings by the Montagnards pose an immediate and very serious problem for the GVN. The Montagnards have a violent dislike for and distrust of the lowland Vietnamese, and have sought autonomy for years. The Vietnamese on their part look down on the Montagnards; until recently, the GVN has usually acted in a manner which has widened rather than lessened the breach between the two. The problem has been further compounded by constant and rather intensive Viet Cong political and psychological agitation among the Montagnards, playing on their aspirations and their dislike of the ethnic Vietnamese. Resentment over the killing of some 70 Vietnamese by tribesmen during their revolt will make it extremely difficult for the GVN to offer settlement terms acceptable to the Montagnards. Thus, there will probably be continuing disorders in the Highland areas, diminishing cooperation with the GVN, and increasing Viet Cong influence.

8. *Offsetting Considerations.* Although the signs of deterioration are many and clear, there are offsetting considerations that reduce the likelihood of sudden collapse and afford some very slim hope that the trend can be arrested. The Vietnamese people have a long record of resilience in the face of adversity; the ability of the peasants and even of urban elements to continue normal patterns of life despite political disorder makes for some degree of basic stability. The routine functions of government still work fairly normally; business does go on; and the streets are not places of constant terror. Discouragement over the absence of leadership and the progress of the war has not yet led to calls for ending the fighting. Few if any of the many groups now seeking to enlarge their powers regard an accommodation with the Communists as consistent with their interests. Finally, the military instrumentalities of pacification still exist and retain significant capabilities.

9. *Tensions in US-GVN Relations.* In the last month or so, there has been a disturbing increase in anti-American sentiment at various levels of Vietnamese society. Recent demonstrations in Hue, Da Nang, Qui Nhom, and Nha Trang have had definite anti-American overtones. These were probably attributable in part to Viet Cong agitation and incitement, but in some measure they seem also to have reflected a genuine irritation at the Americans

for various reasons having no direct connection with Viet Cong activity. For its part, the Buddhist leadership, whether anti-Communist or not, is imbued with intense nationalism which has at times manifested itself in opposition to US policies and actions. Suspicion of US motives and concern over US involvement in internal policy is growing among the top echelons of the GVN, and, most importantly, on the part of Khanh himself.

10. *GVN Contacts with the Communists.* The principal GVN leaders have not to our knowledge been in recent contact with the Communists, but there has been at least one instance of informal contact between a lesser governmental official and members of the "National Liberation Front," which is a creation of Hanoi. Moreover, there are numerous potential channels of communication between the present GVN leadership and the DRV authorities, and these could very likely be used without US knowledge.

11. *Coup Possibilities.* Although no definite coup plans are known to be afoot at the moment, we believe that further coup attempts are likely, given the ambitions, discouragement, and bitterness prevalent among certain key South Vietnamese military and civilian figures—and the comparative ease of mounting a coup attempt in the present deteriorating scene.

12. *Alternatives to Present GVN Leadership.* Present plans call for the establishment of a new, broadly based, and predominantly civilian government by the end of October. Such a government might do better than the present one, but the odds are against its having the cohesion and effectiveness necessary to arrest the current decline. No visible alternative seems any more promising. Indeed, we cannot presently see any likely source of real leadership; no Magsaysay has yet appeared. None of the military personalities and factions seems capable of commanding a sufficiently broad spectrum of support. Of nonmilitary figures, the Buddhist leader Tri Quang is the strongest political personality and has demonstrated talents for leadership and organization. But he apparently desires to avoid such responsibility, and a Tri Quang government would face strong opposition from militant Catholics, some of the military, and certain other groups. Not least, it would be a difficult government for the US to work with, and some of its major policies would almost certainly not be consonant with US interests.

The Viet Cong

13. *Viet Cong Policy.* There are numerous signs that Viet Cong agents have played a role in helping sustain the level of civil disorder which has recently prevailed in the cities of South Vietnam; they have also affected the tone and direction taken by some recent protest demonstrations. Their hand was evident in the recent riots in the capital of Binh Dinh Province, and they may have already penetrated the PRC. Viet Cong propaganda throughout September has increasingly called upon the people to take advantage of the government's confusion by pressing on all fronts. This capitalizing on unrest is an old policy; what is new is the rich opportunity presented by the collapsing of GVN authority. The Viet Cong have apparently decided that heightened efforts on their part will reduce the country to near anarchy and the government to impotence, bringing an early victory in the form of a negotiated truce and a "neutralist" government dominated by their National Liberation Front. Although these heightened efforts may include some battalion-sized, or larger attacks, we do not believe that the Viet Cong are trying to force a military decision at this stage. Rather, they will continue stressing small-scale terrorist activity aimed at furthering the breakdown of administration and the decline of faith in the government.

14. *Viet Cong Capabilities in the Cities.* Viet Cong strength in the cities has almost certainly increased substantially in recent months. We base this conclusion on our general reading of the present situation rather than on specific knowledge of current Viet Cong assets. In the closing days of the Diem regime, Vietnamese police and security agencies had a fairly good reading on the nature and extent of the Viet Cong apparatus in the capital area, and it did not constitute a serious threat at that time. Immediately following the November 1963 coup, however, Colonel Tran Ba Thanh became Deputy Director of National Police. There are strong grounds for believing that Thanh may be a Communist agent; in any event he released some key Viet Cong prisoners, destroyed Viet Cong dossiers in police archives, and placed at least one known Viet Cong agent in a key position within the police structure. Although Thanh was ousted when Khanh seized power, the Saigon police and security services have not recovered their anti-Communist capabilities. The fact that Communist agitation still remains under careful cover, however, suggests that the Viet Cong intend still to husband these assets and not risk them in a premature takeover attempt.

NATIONAL INTELLIGENCE ESTIMATE 53-71
29 APRIL 1971
SOUTH VIETNAM: PROBLEMS AND PROSPECTS

NOTE

The US military presence in South Vietnam will be reduced to about 185,000 by the end of 1971 and even further by the end of 1972. But it is assumed in this paper that a US military support effort will be maintained beyond 1972 along with substantial amounts of US economic assistance. As the US disengages militarily, however, the noncommunist forces in South Vietnam will face the test of dealing with a variety of challenges largely on their own. This Estimate assesses the major problems which will confront the Saigon government in the future as the US reduces its presence and which, depending on how they are met, will largely determine South Vietnam's prospects through the mid-1970s.

CONCLUSIONS

A. The outlook in South Vietnam for the remainder of 1971 is reasonably good. The past three years have produced a more stable political situation, a marked improvement in security conditions, and considerable progress in Vietnamization. Meanwhile, communist problems in supporting the insurgency have mounted. Though communist military strength remains substantial, particularly in the northerly provinces, most of the available evidence suggests that—for the next six months or so—they will continue to rely essentially on the basically conservative tactics observed over the past year. While occasional spurts of larger scale military activity seem almost certain, particularly in the north, any such activity in South Vietnam would probably be limited in area and duration.

B. On the political front, the odds in the presidential election of October 1971 appear to favor a Thieu victory. His re-election would, of course, constitute a mandate for continuing to oppose the communists along present lines. But even the election of the more equivocal "Big" Minh would not necessarily lead to any major shift in Saigon's approach to the struggle, if only because the South Vietnamese military would compel Minh to be extremely circumspect in any dealings with the communists. As for Hanoi, the defeat of Thieu would provide a tempting opportunity to feel out South Vietnamese sentiment on continuing the war.

C. Prospects for 1972 are less clear. The approaching US election period, coupled with continued drawdowns of US troop strength in South Vietnam, make it probable that Hanoi will elect to step up its military activity by early 1972. We do not envisage an effort to duplicate in scale or intensity the 1968 Tet offensive. We would expect a general increase in the level of communist activity with sharp focus on a few selected areas, most likely the northern provinces and highland region of South Vietnam. The aim of this strategy would be to score tactical victories likely to impact adversely on the South Vietnamese and US will to persist in the struggle—specifically, to discredit the Vietnamization program and to encourage sentiment in the US for complete disengagement from the war. There are practical limits, however, to what the communists could accomplish militarily next year in South Vietnam, and we do not believe that they will be able to reverse the military balance there.

D. At the same time, there seems little doubt that the communists will continue to maintain an active military and political challenge to the GVN well beyond 1972. The

question in their mind is how and at what level the campaign should be prosecuted. Much would depend on Hanoi's view of the remaining US presence and commitment to Saigon, and on what balance Hanoi struck in its willingness to continue investing resources in the struggle. There are risks and practical difficulties in any course which Hanoi might contemplate: an effort to exploit the drawdown of US forces by a return to large-scale military action; to continue a course not unlike that of the past two years; or to pursue a purely guerrilla struggle at a much lower level. In any case, as it views developments in Laos and Cambodia, Hanoi may well calculate that it can maintain forces on South Vietnamese borders as long as necessary to sap Saigon's will to continue the struggle.

E. In attempting to cope with the communist military threat, South Vietnamese forces will probably require substantial US support for many years. ARVN lacks the logistical system and technological and managerial skills required to maintain and support a modern fighting force. There are also serious personnel problems, including a shortage of qualified leaders and a propensity for enlisted ranks to desert. Problems of leadership and morale are even more severe in the territorial forces and village militia, key elements in the campaign to control the countryside.

F. A major element in Hanoi's ability to stay the course in South Vietnam is the apparent durability of the communist party apparatus there. The apparatus has been hurt, severely in some areas, but relatively few high-level communist cadres have been eliminated as a result of direct GVN action against them. The communists have been able to maintain a viable organization, and this is likely to continue to be the case for the foreseeable future.

G. In addition to the threat posed by the communists, the GVN will have to cope with internal problems. These include meeting the increased demands of a society in the process of change. A greatly enlarged urban slum population has been created and is a target for radical agitation, while the rural populace looks increasingly to the government to meet its growing needs. In the economic sphere, the GVN simply will not be able to satisfy the demands of this "revolution of rising expectations" from its own resources. The political impact of the changing South Vietnamese society is less easily defined. But the regime is likely to find itself faced with rising nationalism, often manifested as anti-Americanism. In the future, there is also likely to be a shift toward a more traditional Vietnamese pattern of a centralized executive authority, although the major elements of the present constitutional system are likely to be retained. Such a system might result in a more efficient government, but the regime might also rely increasingly on its coercive powers, thereby leading to instability and risking political disintegration.

H. Over the longer term, a critical factor in South Vietnam's survival will be the will of the South Vietnamese as a people and as a nation to sustain the struggle against the communists. As Vietnamization proceeds, the South Vietnamese will have to cope with the communists and face the country's problems largely on their own. Developments thus far suggest that they are responding reasonably well to the challenge. But there is no way to determine how tenacious they will be a few years hence when the US is much further along the road to disengagement.

I. Thus, it is impossible at this time to offer a clear-cut estimate about South Vietnam's prospects through the mid-1970s. There are many formidable problems and no solid assurances over this period of time. In our view, the problems facing the GVN, the uncertainties in South Vietnam about the magnitude, nature, and duration of future US support, doubts concerning the South Vietnamese will to persist, the resiliency of the

communist apparatus in South Vietnam, and North Vietnam's demonstrated ability and willingness to pay the price of perseverance are such that the longer term survival of the GVN is by no means yet assured.

DISCUSSION

I. The Present Situation

1. Over the past three years, South Vietnam has made substantial progress. The performance of the army (ARVN) has improved steadily; it has assumed the bulk of the ground fighting responsibility without any appreciable decline in territorial security. Indeed, in this period, the Government of South Vietnam (GVN) has extended its control, or at least its access, to most of the country's territory and almost all of its population. As a result, people's confidence in the government has increased, particularly in the rural areas.

2. A more stable political situation has also evolved in South Vietnam. Political participation has broadened greatly, and all major groups have at least a piece of the action—if not in the executive branch, then in the legislature or at the local level. The regime apparently values the aura of legitimacy that accrues from operating on a constitutional basis, and most political elements, including the key military leaders, show no disposition to challenge the government frontally. To most groups, the gains to be derived from working within the system appear to outweigh the costs and risks of efforts to overturn it. In addition, the government's administrative structure has improved, making possible a more vigorous and effective attack on the country's problems. Overall, there is considerable forward momentum in South Vietnam today, and an air of cautious optimism permeates many sectors of the population.

3. As for the Vietnamese communists, during the past year their military/political position in the countryside has been further eroded, considerably in some areas, and their forces have continued to suffer substantial casualties despite lower levels of combat activity. Captured documents continue to reflect difficulties in the communist effort to strengthen the party's control apparatus. Nor has Hanoi been able to achieve decisive results on the political front. Despite surges in antiwar sentiment in the US, the administration has been able to pursue Vietnamization at a deliberate pace, thus dimming any hopes that Hanoi may have had of winning concessions from the US in the near term. The turn of events in Cambodia and southern Laos has compounded communist problems in South Vietnam, requiring Hanoi to divert energy and manpower toward reconstituting and expanding logistical routes. The loss of sanctuaries and the widened area of conflict have particularly complicated the communist situation in South Vietnam. Hanoi also has problems on the home front, where economic reconstruction and development continue to be subordinated to the requirements of the war. Morale problems have resulted as manpower losses in the South have increasingly been brought home to the North Vietnamese populace.

4. But the war is far from over. Despite their difficulties, the communists retain important military capabilities throughout Indochina. As their recent performance in southern Laos demonstrates, they can still fight hard when they choose to do so. Meanwhile, the tightly disciplined communist party organization in South Vietnam gives them considerable flexibility in adapting to changing conditions. Finally, as the US withdraws, existing weaknesses in South Vietnamese government and society will tend to surface, requiring increased attention in Saigon to basic problems affecting internal stability and national development.

II. GVN Problems and Prospects Through 1971

A. POLITICAL PROBLEMS—THE OCTOBER ELECTION

5. As the next order of business, the South Vietnamese must settle the question of national leadership for the next several years. This process will come to a head in the presidential election now scheduled for October 1971.[1] The election will test public acceptance of Thieu's stewardship and, to some degree, the strength of the system of government now prevailing in South Vietnam.

6. The Thieu government's image with the electorate is at best gray. Inability to bring peace, the military's large role in government, corruption, economic problems, and the GVN's extensive dependence on US support all will cost Thieu votes. Even so, Thieu seems to be the front runner at this time. He has, first of all, tremendous assets at his disposal. Thieu can utilize available governmental and military personnel and funds to propagandize for his candidacy and to get out the vote. His control of the massive governmental administrative and security apparatus and his personal support within the military establishment probably assure him a large number of votes from these sectors. Finally, he has worked hard in recent years to broaden his appeal to the rural population; the land reform program and the improved security conditions in the countryside should serve to bolster his standing among the peasantry.

7. *Thieu's Opposition.* Thieu's major opponent currently appears to be Duong Van ("Big") Minh, though he may ultimately decide not to run. Minh's appeal has never been tested at the polls, but he is a national figure and appears to have a favorable image throughout much of the country. And despite his ineffective performance during his three months as Chief of State (1963–1964), Minh apparently retains some support within the military and administrative establishments. The An Quang Buddhists, despite certain reservations, are also likely to throw their considerable influence behind his candidacy. Although he is neither a "peacenik" nor anti-American, Minh would probably pull a substantial proportion of the pro-peace and anti-US vote. More important, Minh should also gain the bulk of the anti-administration protest vote. Finally, Minh might be the recipient of whatever votes the communists could deliver, though there are no indications that they believe Minh would wittingly serve communist ends.

8. Minh so far has stuck to platitudes about national unity under his leadership; his stand on major issues has been vague. He blames Thieu for inflation in South Vietnam, but has not indicated how he would handle the problem. He has identified himself more or less with groups espousing peace sentiments, but he has not come forth with any specific proposals for settlement of the war. He seems to believe that he could outmaneuver the communists and has adopted a less bellicose stand than Thieu against their participation in the political process, but he has ruled out the possibility of a coalition arrangement. He has been in contact with most major political elements in South Vietnam, but has made no firm commitments to any. Many people, including some of his supporters, have reservations as to whether Minh will run and whether he could provide adequate leadership, especially in the period when the US is withdrawing from South Vietnam.

---

[1] Elections for the Lower House will take place in August. Although these elections may provide clues to the way the political winds are blowing in South Vietnam, they are more likely to reflect local issues and personalities.

9. Vice President Nguyen Cao Ky is also a potential candidate. Although he has not officially declared himself in the race, he is casting about for political support and is increasingly vocal in his criticism of Thieu and his policies. Ky, however, does not appear to have a major power base or a large popular following and would appear to have little chance of winning the election. Thus, it is possible that his current maneuvering is designed to enhance his bargaining power and that he will not actually run. But if he does, Ky's candidacy will be a complicating factor in the election. He would probably cut into Thieu's support among the military; since he seems to be trying to project a somewhat "dovish" image, Ky could also draw some support away from Minh.

10. *The Communist Role in the Election.* The communists would certainly like to see Thieu defeated or at least to discredit the election results in South Vietnam. It is doubtful, however, that they have the capability to do very much either to influence the election's outcome or to disrupt the voting process on a countrywide basis. Their past performance in this area has been weak, and captured documents suggest that their shortcomings have not yet been overcome. Thus, while the communists would attempt to exploit any anti-regime demonstration that occurred, it is doubtful that they could spark significant demonstrations on their own. Beyond this, Hanoi might surface a "peace" initiative during the campaign in an effort to complicate Thieu's position.

11. But in general Hanoi seems to assume that Thieu will be re-elected and is already denouncing the elections as a fraud. Even if Minh won, the communists probably would not view his victory as portending a decisive shift in the political climate in their favor. Communist hopes in the event of a Minh victory would probably rest more on an expectation that the GVN would be more inefficient and unstable under his leadership than on a belief that he would be conciliatory. They might feel out Minh's intentions, however, by adopting a less bellicose attitude toward the new government and perhaps by showing a somewhat greater interest in talking with Minh.

12. *Election Prospects.* Uncertainties as to trends in the overall military situation over the next few months complicate an election forecast. If, on top of Lam Son 719, the communists maintain a considerable show of military strength over the next few months, Thieu's election prospects might be affected adversely. On the other hand, a generally low level of communist military action during this period could enhance the regime's claims to progress in the military and security fields, and increase Thieu's support in the election.

13. Another factor in the election campaign will be the South Vietnamese perception of the US posture. Paramount in the minds of many South Vietnamese is the question of whether the election results would significantly affect the level of US support. Most South Vietnamese believe that the US favors Thieu staying in office, and this may incline many voters to opt for him in hopes of ensuring continued US support. Aware of such sentiment, Minh has gone to some lengths to urge a policy of "neutrality" for the US in the election, stating that unless the US demonstrates that it favors no particular candidate, he may not even run since Thieu would be sure to win. In any event, if the South Vietnamese public came to believe that the US was truly neutral or favored someone other than Thieu, his chances of election would probably decline.

14. All things considered, however, Thieu appears to stand a better than even chance of winning the election. His control of the governmental apparatus and the financial resources at his disposal are advantages difficult to overcome. This knowledge should encourage discretion on his part and reduce the possibility of blatantly underhanded election tactics by the regime. For their part, despite a desire to unseat Thieu, most of the

noncommunist opposition elements would probably be loath to risk undermining the present system by disruptive actions.

15. If Thieu is re-elected, it will be an obvious mandate for continuing along present lines. But Minh also might not depart significantly from existing policies. He would face the same problems with basically the same assets as Thieu; and, ultimately, he would have to rely on the military as the major prop of his regime. There would be a chance of erosion in governmental effectiveness under Minh as he attempted to put his stamp on the administration, mainly because this would almost certainly entail a shake-up in personnel assigned to key programs. Minh's policies toward the communists, however, would be the key factor in his hold on power once elected. If he began to assume what the military deemed an overly accommodating posture toward the communists, they would probably warn him to desist; a coup would be possible.

16. Previous elections under the Thieu regime have appeared to be relatively honest. But the stakes are higher than ever before. The country's future is likely to be determined by developments during the next four years, a period in which the South Vietnamese will have to demonstrate that they can fend largely for themselves as the US progressively disengages from Indochina. This could increase the regime's nervousness about the Minh candidacy. Ky's appearance on the ballot would increase the uncertainty in Thieu's camp. The regime might conclude that a relatively honest election was too risky and be tempted to rig the voting. If they did so in a blatant manner, it could inflame the political opposition and special interest groups, and the regime might find itself faced with demonstrations and rioting, especially in the cities. Such developments obviously would lessen the prospects for national cohesion over the longer term.

B. ECONOMIC PROBLEMS

17. With the help of large infusions of US economic assistance, the South Vietnamese economy has responded relatively well to years of war and military mobilization. Per capita consumption has remained approximately stable, and there has been no serious decline in domestic production despite the massive dislocation of the labor force. In addition, as a result of military construction activities, South Vietnam now possesses a well-developed transportation network and air and port facilities. In the past few years, the agricultural sector has benefited from technological advances, and a revolutionary land reform program has gotten underway.

18. Nevertheless, there are still serious shortcomings in the South Vietnamese economy. It is far from being self-sustaining; large-scale US assistance provides the basic underpinning for the economy and will have to do so for years to come. And GVN economic policies have perforce largely been concerned with the short-term military and political consequences of the war, and have slighted the more basic aspects of economic development.

19. Over the short term, the major problem continues to be the threat of inflation.[2] Although the regime's recent economic reforms contributed to a substantial slowdown in the pace of inflation, it is a persistent and serious problem. At its heart is the massive

[2] The increase in prices ranged from 30 percent to 55 percent each year from 1965 through 1969 and amounted to 30 percent in 1970. Since July 1970, however, there has been almost no increase in basic prices.

spending by the Vietnamese and US Governments for war-related purposes. As a result, effective demand has tended to exceed the available supply of goods and services. Only by recourse to a program of massive imports, financed almost totally by the US, has the GVN been able to keep inflation from skyrocketing.[3] The availability of imported consumer goods has improved the GVN's image at home, but at the same time it has conditioned the population to expect relative abundance in the midst of war. In short, consumer demand has become rather sophisticated, while the GVN's economic base and practices, despite some improvements, have not.

20. The US troop withdrawal program will tend to complicate the effort to find solutions to the GVN's economic problems. Large numbers of South Vietnamese workers are being released by US forces and their contractors. Providing additional jobs in the civilian economy would require increases in production and imports, which in turn would require increased foreign aid. Meanwhile, the reduction in US military expenditures is reducing the GVN's supply of dollars, and hence its own resources for purchasing imports and stimulating economic growth.

21. *Short-Term Economic Prospects.* Income distribution will continue to be an important issue in South Vietnam. In recent years, farmers have had a significant increase in real income, but the political will to tax the farmer directly does not seem to exist. Within the urban areas, workers in the private sector have done reasonably well despite some erosion of real income. On the other hand, the civil service and military are much worse off than several years ago despite a recent wage increase, and their unhappiness could create problems for the government in addition to making any systematic attack on corruption vastly more difficult. Despite this, the GVN probably will not attempt to redistribute income significantly through another government pay hike or by other means in this election year.

22. Grievances growing out of the maldistribution of income may cause political difficulties for Thieu in the months ahead, but are not likely to pose a critical threat to the GVN's viability during 1971. The worst of the regime's other economic problems will continue to be alleviated by large-scale US assistance. Labor dislocations caused by US withdrawals will create some localized problems, but these are not likely to be critical.

C. MILITARY PROBLEMS—COMMUNIST STRATEGY AND UNITED STATES' WITHDRAWALS

23. *Communist Military Action in the Near Term.* The communists retain significant military capabilities in various parts of South Vietnam, particularly in the northerly provinces. But in southern South Vietnam, these capabilities are severely limited relative to the period 1967–1969 as a result of the loss of the Sihanoukville supply route, disruption and attrition of the communist support structure in South Vietnam itself, continued air interdiction, and allied cross-border operations in Cambodia and Laos. The communists recognize their weaknesses in South Vietnam and over the past year have been trying to

[3] From an annual average of $334 million during 1963–1965, imports of goods rose to an average of $725 million during 1966–1969. On the other hand, exports declined rapidly because of reduced production of the country's two major export commodities—rice and rubber. In 1969, exports amounted to only 4 percent of imports; data for 1970 are not available.

repair the situation. Heavy emphasis has been given to beefing up the infrastructure, increasing the number of "legal" communist cadres who can operate in GVN-controlled areas, and subverting the South Vietnamese military and security forces. In the meantime, the communists have relied largely on small unit actions, terror tactics, and sabotage in an effort to conserve forces in anticipation of a prolonged struggle.

24. Most of the available evidence suggests that, for the next six months or so, the communists will continue with these same basic tactics to husband manpower and resources and to rebuild their position in the countryside. Nevertheless, occasional spurts of communist military activity will occur and there may be some military pyrotechnics prior to the South Vietnamese presidential election. But the present pattern of communist action in most of the country, the state of readiness of their forces in South Vietnam, the restrictions imposed by their logistic support capability, and the evidence drawn from captured documents, clandestine reports, and interrogation of communist prisoners and ralliers all suggest that any heightened military activity in South Vietnam over the next several months will be limited in area and duration.

25. *Impact of US Withdrawals.* South Vietnamese forces are being spread more thinly with each succeeding US withdrawal, and despite the weaknesses of communist forces, there will probably be some deterioration in local security during 1971. The combat effectiveness of ARVN may also suffer somewhat as US artillery and helicopter support is diminished. But for the next several months at least, no critical problems are likely to develop. So far, the psychological impact of the withdrawals has been limited; most South Vietnamese have by now adjusted mentally to the fact that the US will continue to scale down its military involvement in Vietnam. Even though demonstrated ARVN shortcomings may raise doubts in South Vietnam about ARVN's ability to fill the gap over the longer term as the US disengages from Indochina, such doubts are unlikely to result in any serious deterioration in the morale of ARVN or the general public during 1971.

III. Major Problems Over the Longer Term

A. THE NATURE OF THE COMMUNIST THREAT

26. *Prospects for* 1972. Hanoi's approach to the war in 1972 will be conditioned by certain basic elements in the situation such as continued US withdrawals, improvements in the pacification situation and in the capabilities of South Vietnam's military forces, and communist determination to gain control of South Vietnam. Certain recent developments, particularly allied operations in Laos and Cambodia, will also have some effect. On the one hand, the communists suffered heavy casualties in these operations, lost and expended significant quantities of supplies, and had their supply lines disrupted; and this is likely to impose restrictions on the scale of military action possible during the early stages of the 1971–1972 dry season. Beyond this, allied action or the threat of action in Laos and Cambodia will impose a continuing burden on Hanoi to protect and maintain the Laos supply route.

27. On the other hand, having weathered the recent ARVN cross-border operations in southern Laos, Hanoi probably feels somewhat more confident that it can wait out the withdrawal of US forces and stay the course in Indochina. Hanoi's view is probably tempered by the realization that communist forces suffered very heavy casualties in Lam Son 719 and benefited from terrain which favored the defense, as well as from superior numbers in place on the ground. The operation did not provide any solutions to the many

problems the communists face in South Vietnam. But from Hanoi's point of view, its forces contained a threat to its vital supply lines, and avoided a critical setback to the 1970–1971 supply effort. Hanoi probably calculates that ARVN, on its own, would have great difficulty in mounting further cross-border operations of this magnitude once the US is largely out of the picture.

28. Given this outlook, Hanoi might opt in 1972 for a continuation of its basically low-profile military approach in South Vietnam. In the meantime, the communists would pursue their efforts to prepare the logistical and organizational base necessary for either a long drawn-out struggle or a return to large-unit action once US forces were no longer an important factor in the war.

29. But there are other considerations which could lead Hanoi to attempt a step-up in military activity in 1972. For example, if communist fortunes took a sharp turn for the worse in the months ahead, Hanoi might hope to reverse the trend by increasing its attacks against ARVN and other government security forces during the 1971–1972 dry season campaign. Such a decision on Hanoi's part could also come later in 1972 if Hanoi at that time were convinced that the US was determined to maintain an effective residual presence in South Vietnam for an extended period.

30. Regardless of the course of the war, Hanoi's leaders might see considerable advantage in a show of military muscle prior to the US election, intended to demonstrate that Vietnamization was not working and to fan antiwar sentiment in the US. In their view, the effort could help generate increased domestic pressure on the US Administration to disengage completely from the war or, failing this, it might affect the election outcome itself. They might also calculate that the backlash in South Vietnam from negative US reactions to adverse battlefield developments would work to communist advantage by sharpening US-South Vietnamese differences.

31. On balance, we believe that Hanoi will find the arguments for some step-up in its military activity in South Vietnam persuasive. But this would be likely to differ from Hanoi's present strategy more in degree than in kind. Thus, we would not envisage an effort by Hanoi to duplicate in scale or intensity the 1968 Tet offensive. Instead, we would expect a general increase in the level of communist activity with sharp focus on a few selected areas, most likely the northern provinces and highland region of South Vietnam. The thrust of this strategy would be to attempt, with greater determination than in recent years, to score tactical victories aimed at impacting adversely on the South Vietnamese and US will to persist in the struggle.

32. Whether or not the communists initiate such increased activity, we do not believe that they will be able to reverse the military balance in South Vietnam in 1972. Continuing communist difficulties will impose limits on how much they can accomplish, and continued allied pressures during the remainder of 1971 and pre-emptive operations in the 1971–1972 dry season could forestall communist preparations for extensive military operations. But the communists are unlikely to be frustrated at every turn; there are too many vulnerabilities in the South Vietnamese situation. For example, the adverse psychological impact in South Vietnam of increased communist military activity could be considerable, particularly if it led—or were thought by the South Vietnamese to be leading—to a weakening of US resolve. And even if—in a purely military sense—the odds seem to favor the South Vietnamese being able to contain the communist effort in 1972, the GVN will still be faced with a communist military and political organization retaining significant strength and potential.

33. *Beyond 1972.* At this point in time, there seems little doubt that the communists will continue to maintain an active challenge to the GVN well beyond 1972. Despite continued concern over the Sino-Soviet dispute, Hanoi probably assumes that it will continue to receive military and economic assistance from both Moscow and Peking as long as necessary. For its part, Hanoi has committed enormous manpower and material resources and has suffered staggering losses in attempting to gain control of South Vietnam. And while there have been shifts in strategy, Hanoi's will to persist has shown little indication of flagging. The war has been going on for over a generation—it has become a way of life for the communists and a part of their ethos. Any leader in Hanoi who advocated giving up the struggle would risk losing his position. Indeed, the present communist leadership might find it difficult to contemplate any course other than continuation of the struggle even if it meant throwing away additional resources in a basically fruitless effort. The question in their minds is not whether to continue the struggle, but how and at what level it should be pursued.

34. The "how" and "at what level" may be as difficult for Hanoi to decide as it is for us to estimate at this stage. Much would depend on how Hanoi viewed the remaining US presence and commitment to Saigon, on the strength and morale of ARVN at that time, and on what balance Hanoi struck in its willingness to continue investing resources in the struggle. There are risks and practical difficulties in any course which Hanoi might contemplate.

35. Assuming that ARVN and the territorial forces maintain or improve their capabilities over the next year or so, any communist effort in the period beyond 1972 to return to large-scale military action in South Vietnam would involve heavy manpower commitments and other strenuous demands on a North Vietnamese population already weary from the cumulative effects of the war. It would also require, as a precondition, the maintenance of secure logistic routes to the South and the rebuilding of an infrastructure in South Vietnam capable of supporting the operations of main force units in the countryside. And, of course, a large-scale military effort might fail and put at risk the ability of Hanoi to rebuild its forces once again.

36. To do too little also involves serious risk. There is no way to be sure what the impact of a long, drawn-out, low-level struggle would be on communist cadres and lower level elements in South Vietnam. Many of them might in time abandon the effort, rendering the communists unable to present a credible challenge to local security in South Vietnam. In North Vietnam, the communists might also face a decline in popular commitment to the struggle. In a sense, the war is an "old man's" war, and whether the younger generation in the North shares the same unswerving dedication to the reunification of Vietnam as their elders cannot be determined.

37. The communists may conclude that their circumstances at home and in the South leave them little choice but to pursue a middle course, one not unlike that of the past two years. This would mean that the GVN would be faced with a continuing threat from some main force units, particularly in Military Regions (MRs) I and II, and a generalized local security threat posed by highly self-sufficient guerrillas, sappers, and terrorists throughout the country. And the political, psychological, and subversive struggle would go on at all levels of society.

38. Hanoi can also hope that developments in Laos and Cambodia will further communist objectives in South Vietnam in the years ahead. The communist position in both countries, particularly Laos, is stronger than in South Vietnam. In Laos, Hanoi

probably calculates that Vang Pao's Meo guerrillas are fading as an effective fighting force; this, coupled with the possibility that the US air role in Laos may be reduced, could lead Hanoi to foresee the end of any effective indigenous resistance in Laos to communist aims. In Cambodia, on the basis of performance, the communists probably foresee little threat to their established positions from Phnom Penh's fighting forces. Thus, Hanoi probably believes that its prospects over the longer term of being able to hold the key logistical routes extending through the Laotian Panhandle and northeastern Cambodia into South Vietnam are good. And it may calculate that even a moderate level of activity in South Vietnam coupled with the permanent threat posed by communist control of the border areas would in time sap the South Vietnamese will to continue the struggle. At a minimum, Hanoi would expect this situation to impose heavy additional burdens on South Vietnamese forces, both in protecting the country's long border and in doing the work of indigenous anticommunist forces in southern Laos and Cambodia, all the while filling in for departing US forces in South Vietnam.

B. GVN CAPABILITIES TO DEAL WITH THE COMMUNIST THREAT

39. *Military and Security Forces.* As the US scales down its involvement in the war, the South Vietnamese military forces will be required to assume increasing responsibilities in the struggle against the communists. Given in political requirement to provide security to the population throughout large portions of the countryside, the GVN will be forced to maintain a large military establishment to check communist activity. Progress has been made in preparing the South Vietnamese forces for the time when they are more or less on their own, but it will be years before the South Vietnamese can be self-sufficient in the military field.

40. For example, although the South Vietnamese have a significant capability for in-country air support, plans are only in the embryonic stage to provide them with a capability to mount air interdiction efforts against the communist logistical network in southern Laos. Further, ARVN has come to rely on helicopter support, and current plans call for a major reduction in the number of helicopters to remain in South Vietnam as US forces depart. Despite substantial improvements, the GVN's logistical system is not yet capable of meeting the large military establishment's needs without relying heavily on US assistance. Similarly, it will be many years before the South Vietnamese military acquires the requisite technological and managerial skills to handle the complexities of maintaining and supporting a modern fighting force.

41. The availability of technical and logistical assistance will be especially vital to the maintenance of ARVN's fighting effectiveness. ARVN has become increasingly dependent on the availability of such complex equipment as helicopters, advanced communications and fire-control equipment, and electronic monitors and sensors. The use of such equipment has given the South Vietnamese considerable advantages in combating the communists. But without substantial US assistance in maintenance, much of the modern equipment would probably deteriorate over time. ARVN might find it difficult to change its tactics and to fight without all of its technically sophisticated paraphernalia. The South Vietnamese will look to the US to continue to provide—and to assist in maintaining—the types of equipment presently available.

42. The persistence of certain basic shortcomings within the South Vietnamese military establishment is likely to impede military progress over the longer run. Despite

improvements, there is little prospect that the military leadership will lose its elitist cast; high-level promotions are likely to continue to be based more on social class and personal loyalties than on military competence. Life for the common soldier will continue to be hard, and separation from families will be frequent. Military pay and allowances at all ranks, already very low, probably will not keep up with the pace of inflation. Under these conditions, military desertions are likely to continue at a fairly high rate.

43. Problems of leadership, morale, and material support are even more severe in the territorial security forces (Regional Forces and Popular Forces—RF/PF) and in the People's Self Defense Force (PSDF) than in the regular military branches. This is so even though these forces are now performing well in many parts of South Vietnam and deserve much of the credit for the improvement in local security. As the US withdraws, ARVN will have to assume the full burden of the main force war, leaving local security even more fully in the hands of the territorial forces and the PSDF. The critical importance of these forces appears to be understood at the highest levels of government, and they are receiving better training and equipment. But a considerable part of the pressure to improve the local units has come from the US. Only with a continued push from the highest national levels will the territorial security forces be assured the equipment and support needed to assume increased responsibilities. Without this support, the GVN's position in the countryside would probably suffer gradual deterioration.

44. Corruption could also continue to impair the military effectiveness of the GVN in the future. Many, possibly most, of the upper echelons of the military establishment engage in some form of corruption; in some cases, the abuses are flagrant and common knowledge. Such excesses tend to lower morale within the ranks and may contribute to the poorly paid, lower level soldier's lack of commitment and tendency to desert. The abundance of US goods has contributed to the growth of corruption and to the improper diversion of military goods and supplies. As the US scales down its effort, such diversions could leave some units short of needed supplies and vulnerable to communist attack.

45. A final critical factor in considering the GVN's military and security forces is that of will. There are no precise guidelines with which to measure the will of the South Vietnamese fighting man. To the extent that they have positive motivation, the RF, PF, and PSDF probably are fighting more from a desire to protect family and village than from any commitment to the Saigon government or aversion to communism. Within the ARVN, many senior officers and noncoms appear ideologically opposed to the communists. Moreover, while most soldiers would like to see the war come to an end, they would certainly prefer that South Vietnam remain non-communist. In general, however, the commitment of ARVN to the struggle rests more on the force of discipline and being caught up in the system than any other factor.

46. *The Attack on the Communist Apparatus.* The GVN's ability to eliminate the communist party structure is questionable. The communist apparatus has been hurt, severely in some areas, but most of the damage stems from the expanded GVN military presence in the countryside and from attrition resulting from the fighting. GVN programs against the communist apparatus have had limited success; relatively few high-level communist cadres have been eliminated as a result of direct GVN action. Moreover, much of the impetus in the GVN's effort has come from US involvement in the programs. As the US reduces its role in these programs, the GVN is unlikely to take up all the slack, and the effort against the communist apparatus would be likely to decline in effectiveness.

47. The South Vietnamese police forces are ill-equipped to take on the task of rooting out the communist apparatus; their operating procedures are inclined to be erratic, and their motivation appears low. The communists have penetrated the regime's security and police forces, and there is a widespread reluctance among the people to turn in communist cadres to the authorities. Many, perhaps most, South Vietnamese have connections, often family ties, with someone in the communist apparatus. Furthermore, the GVN's detention and judicial systems are lax; when apprehended, communists often go free because of slipshod procedures or the venality of GVN officials. As a consequence, the communists have been able to maintain a viable organization despite the GVN's counterefforts, and this is likely to continue to be the case for the foreseeable future.

C. POLITICAL TRENDS

48. The GVN's political cohesion will be subject to increased stress over the next few years as the US presence with its stabilizing influence declines. Frictions between the executive and the legislative branches are likely to sharpen. Though political groups will expect to participate increasingly in the politics of the nation, there is little prospect for the development of truly nationally-based political parties. It is more likely that the political groupings will continue to reflect various parochial and regional interests. The politics of South Vietnam are likely to remain basically divisive in nature much as in the past. Though these conditions may complicate the development of a cohesive political system, they need not necessarily lead to political instability.

49. In the future, there is likely to be a further shift toward a more traditional Vietnamese pattern: a centralized executive authority which nonetheless permits a considerable degree of popular participation and responsibility at the village level. The major elements of the present, foreign-inspired constitutional system, however, are likely to be retained. Continued dependence on US aid and support will provide one incentive to retain them. Additionally, the constitution tends to bestow an aura of legitimacy on whoever holds the presidency. At the same time, many groups of South Vietnamese have come to view the system as something of a barrier against extreme abuses of executive power.

50. The stronger central control envisaged for South Vietnam might well result in more efficient government; if so, it would probably be acceptable to the majority of the South Vietnamese even if democratic niceties were honored more in form than in substance. But the danger in strong central control, especially if popular political participation were severely restricted, is that it could lead to extremes in coercion, increasing grievances against the system and leading organized groups to take their complaints into the streets. The organization and skills necessary to make authoritarian controls effective have not existed in South Vietnam, and in the event of mounting popular opposition, the risk of a breakdown in public order would be high.

51. In any case, as the US phases down in South Vietnam—particularly if the communist military threat increases—the political role of the military is likely to become more open and active. Though hardly a monolith, it seems apparent that the military will remain the ultimate arbiter of power in South Vietnam; not only is it the only truly nationally organized group, but it contains most of the country's competent administrators. Moreover, as any GVN president will recognize, the government will be more secure with heavy military participation than with the generals relegated to the position of disgruntled

observers or plotters. The withdrawal of US forces, however, will remove some of the inhibitions to extra-legal action by the military. If the problems confronting the GVN became particularly critical or if the generals feared that political leaders were about to make a dangerously soft settlement with the communists, they would be likely to attempt a coup. Before making such a move, however, the military leadership would probably attempt to correct such tendencies by exerting influence within the system.

52. Over the longer term, the GVN will have to face the problems of both developing and coping with nationalism. Nationalism is hardly a new emotion for the Vietnamese; in past centuries, nationalism—bordering on xenophobia—has provided strong cement for the nation in its struggle against foreign invaders. It was the ability of Ho Chi Minh to harness this force that provided the major impetus for the communist movement in the struggle for independence against the French. But the GVN has not and probably cannot, over the next few years at least, develop a sense of South Vietnamese nationalism that could be used effectively in the struggle with the North.

53. The traditional sense of Vietnamese nationalism with its xenophobic overtones, however, is alive and growing in the GVN. This is likely to pose problems for US-GVN relations. For the last decade the South Vietnamese have been forced to rely on the US for survival. Many South Vietnamese have found this dependence humiliating, and there is little doubt that a reservoir of anti-American sentiment exists in South Vietnam. Recent demonstrations, sparked by offenses—real and alleged—against South Vietnamese by US military personnel, have illustrated the volatility of the issue.

54. In the future, many issues will be given an anti-American twist by oppositionists anxious to tag the leadership as puppets of the US. Sensitive to such charges, the GVN will try to demonstrate its independence of Washington. Indeed, the government in many cases will find it convenient to shunt the blame for its own shortcomings onto the US, further feeding anti-American sentiment in the South. In short, the US is likely to be placed more frequently in the role of the villain and charged with being insensitive to the needs and interests of South Vietnam.

D. THE CHANGING SOUTH VIETNAMESE SOCIETY

55. Over the longer term, the government in Saigon will be called upon to contend with other new tensions and anxieties which have developed in South Vietnamese society. Since the fall of the Diem regime, South Vietnam has been undergoing a revolutionary transformation—unanticipated, virtually unreported, and largely without guidance or objectives. Years of gradual adjustment to the stresses of war have led to vast alterations in social organization: the displacement of large populations, the disruption and often the destruction of traditional village life, the breakdown and partial replacement of the traditional class system, and the chaotic growth of urban centers.

56. Striking changes in Vietnamese society are taking place in the countryside. In much of the country, Viet Cong and GVN-sponsored land reforms have tended to undermine the power of traditional provincial elites. Radio, television, the Honda, and other manifestations of modernization are altering the small farmer's way of life; the adoption of even a modest amount of modern farming technology is changing his role and expectations. He sees his prosperity linked to free access to GVN-controlled markets. Moreover, after years of GVN neglect, sometimes benign but often not, the Thieu government has begun to woo the villager. In addition to land reform, local leadership and village

autonomy are being emphasized, and there have been promises of large investments in agricultural development.

57. The political implications of these processes cannot be defined with confidence. The rural Vietnamese are not only exceedingly weary of war and political turmoil, but also considerably more sophisticated about national developments. Thus, although the villager resents GVN corruption and abuses of power, there is reason to believe that he is also more resistant to communist blandishments. If the GVN is moderately successful in meeting rural demands for more effective administrative and economic services, and demonstrates greater overall concern with their personal well-being, it may in time alleviate many of the adversities which the farmers have suffered over the past decade and prevent the countryside from serving as the seedbed for yet another cycle of guerrilla activity.

58. While roughly 60 percent of South Vietnam's population still lives in the countryside, there has been an unprecedented influx into the country's towns and cities. Originally caused by rural insecurity, the migration was accelerated by a belief that economic opportunities were greater in the cities. Though any improvements in security and economic conditions in the countryside—and prospective GVN programs—will draw some back to their home areas, problems of rapid urban growth will not dissipate. Those who remain in the towns will still be crowded into slums, detached from their traditional communal ties, and exposed to various forms of agitation. Underemployment will be a problem, particularly as US labor needs diminish. Over time, city dwellers—especially frustrated middle class elements and veterans—could become considerably more receptive to radical appeals if the government is unable to meet their demands.

59. These changes in city and country will strain the government's relatively limited funds and expertise. The GVN's efforts to meet its "revolution of rising expectations" will also be impeded by a cumbersome administrative apparatus and widespread corruption. Even with the best of intentions, the GVN simply will not be able with its own internal resources to generate the jobs and capital needed to satisfy the level of economic demand (goods, services, and technology) already reached. While the Vietnamese are basically ambitious and hard working, industrialization can come only slowly. And it will be some time before they can export large quantities of agricultural products; in particular, the rubber industry, will take years to recover its former vigor. Moreover, prospects are not good for substantial foreign investment or large-scale economic assistance so long as the conflict with the communists remains unresolved.[4]

E. THE "X" FACTOR: THE QUESTION OF WILL

60. All of the political, military, and economic factors discussed above will be important in terms of South Vietnam's future prospects. Nonetheless, an examination of these elements does not provide any certain answer to the key issue: the will of the South Vietnamese as a people and as a nation to sustain the struggle against the communists. There are times when "will" can be measured with a fair degree of confidence. By the spring of 1965, for example, it was clear that the South Vietnamese had lost the will to persist; only the large-scale intervention of US combat troops saved South Vietnam from a communist takeover. At Tet 1968, on the other hand, it became clear that ARVN—as well

[4] Japan and a few European countries have shown some interest in aiding or investing in South Vietnam, but to nothing like the extent that will be required.

as some significant portion of the population—had developed a sufficient sense of commitment to offer vigorous resistance to the communist offensive. Since that time, this sense of commitment seems to have developed further.

61. The problem remains, however, of determining the extent to which the growth in commitment in South Vietnam derives from and is dependent on a continued US presence. For the past five or six years, the Americans have always been present or readily available with their manpower, materiel, and money to assist with military and economic problems. As Vietnamization proceeds, this will no longer be as true. Vietnamization is already bringing home to the South Vietnamese leaders that the time is fast approaching when they will have to cope with the communists and face the country's problems largely on their own. Developments thus far suggest that they are responding reasonably well to the challenge. But there is no way to determine how tenacious they will be a few years hence when the US is much further along the road to disengagement.

62. Thus, it is impossible at this time to offer a clear-cut estimate about South Vietnam's prospects through the mid-1970s. There are many formidable problems and no solid assurances over this period of time. In our view, the problems facing the GVN, the uncertainties in South Vietnam about the magnitude, nature, and duration of future US support, doubts concerning the South Vietnamese will to persist, the resiliency of the communist apparatus in South Vietnam, and North Vietnam's demonstrated ability and willingness to pay the price of perseverance are such that the longer term survival of the GVN is by no means yet assured.

APPENDIX F

SAMPLES AND EXTRACTS FROM THE *PRESIDENT'S DAILY BRIEF*

Note from the Editor: The *PDB is* the most exclusive and prestigious intelligence product, disseminated only to the president and anywhere from a half-dozen to a dozen senior national security officials (the number has varied from administration to administration). It arrives at the offices of these individuals early in morning and consists of as few as two or three pages or as long as thirty pages or more, depending on the extent of noteworthy news from the day before. In recent years, the *PDB* has been printed on slick paper in four colors, with charts, photographs, and lively prose, all in an effort to keep the reader's attention in a world of multiple information sources. While a member of the Aspin-Brown Commission staff, the editor reviewed multiple copies of the *PDB* on behalf of the Commission to determine the extent to which it "added value" over the *New York Times,* the *Wall Street Journal,* and other public media outlets. The results showed that the document was useful, especially on questions of terrorism, the military capabilities of nations around the world, and events and conditions in closed societies, although the public newspapers and magazines often outperformed the *PDB* in some domains, such as contemporary European politics.

Ten declassified (once top-secret) *PDB*s are presented in this appendix, all from the administration of President Lyndon Baines Johnson. They are followed by two extracts from *PDB*s (also once top-secret), one from the Clinton administration and another from the second Bush administration.

Source: The Johnson administration *PDB*s are from the National Security Archive, George Washington University, Washington, DC; the Clinton administration extract is from the Kean Commission, *The 9/11 Report,* The National Commission on Terrorist Attacks Upon the United States (2004), pp. 128–129; and the Bush extract is also from *The 9/11 Report,* pp. 261–262, with a facsimile of the original document on the National Security Archive Website. The Johnson administration documents were declassified and approved for release in 1993, and the two other extracts in 2004.

THE PRESIDENT'S DAILY BRIEF

1. *President's Daily Brief, 7 Auqust 1965 (4 pp.), declassified 15 July 1993*
   Source: Lyndon Baines Johnson Library (Austin, Texas), National Security File, Intelligence Briefings File, obtained by Dr. William Burr.
2. *President's Daily Brief, 13 May 1967, (1 p. excerpt), declassified 14 May 1993*
3. *President's Daily Brief, 16 May 1967 (2 pp. excerpt), declassified 14 May 1993*
4. *President's Daily Brief, 27 May 1967 (1 p. excerpt), declassified 14 May 1993*
5. *President's Daily Brief, 5 June 1967 (3 pp. with "Late Items"), declassified 14 May 1993* Compare to FRUS version which omits Nigeria at http://www.state.-gov/r/pa/ho/frus/johnsonlb/xix/28058.htm
6. *President's Daily Brief, 6 June 1967 (1 p. excerpt), declassified 14 May 1993*
7. *President's Daily Brief, 7 June 1967 (1 p. excerpt), declassified 14 May 1993*
8. *President's Daily Brief, 8 June 1967 (2 pp. excerpt), first page declassified 14 May 1993, "Late Item" page declassified 6 November 1985*
9. *President's Daily Brief, 9 June 1967 (3 pp.), first two pages declassified 14 May 1993, "Late Item" page declassified 6 November 1985*
   Source for the above 1967 PDB excerpts: Lyndon Baines Johnson Library (Austin, Texas), National Security Council History, Middle East Crisis, Appendix A, obtained by Dr. William Burr.
10. *President's Daily Brief, 1 April 1968 (5 pp.), declassified 21 December 1989*
    Source: Lyndon Baines Johnson Library (Austin, Texas), National Security File, Intelligence Briefings File, obtained by Dr. William Burr.

CENTRAL INTELLIGENCE AGENCY
THE PRESIDENT'S DAILY BRIEF
7 AUGUST 1965

1. Vietnam A Soviet cargo ship, the Polotsk, [a still-classified section missing here] is en route to Haiphong, The ship unloaded military cargo in Indonesia; there is no evidence it is carrying such cargo now.

2. South Vietnam There has been no significant change in the situation at Duc Co in Pleiku Province, where South Vietnamese airborne troops are trying to eliminate Viet Cong harassment of a government paramilitary camp.

3. Communist China The loss of two Chinese Nationalist patrol craft on 5 August in an encounter with Chinese Communist naval vessels off the mainland coast at the southern end of the Taiwan Strait appears so far to be an isolated incident. Before contact with them was lost, one of the Chinese Nationalist vessels reported sinking three "targets," but there is no confirmation. There is no sign of any other significant Communist military reaction to what seems to have been a Nationalist incursion into Communist-controlled waters. (See map)

4. Indonesia [still-classified section here] Sukarno collapsed three days ago and was still in bed yesterday.

Despite Sukarno's long-standing kidney ailment, for which he delays proper treatment, he has seemed quite chipper lately. [Classified section.] [A] team of Chinese

Communist doctors has been scheduled to visit Djakarta and there is some suspicion that another acupuncture treatment may be involved. [Classified section.]

[A]lthough Sukarno may only have the flu, background political maneuvering may already have begun against the possibility it is more serious.

5. Greece The King continues to talk with political leaders. The last word [still-classified section] was that he would delay until Monday announcing his next choice for the premiership, even though he may make his decision today.

The Communist press is playing up a fabricated document purporting to link the US with a tragic explosion last November at a Communist-sponsored celebration. This is an obvious effort to discredit pro-US elements during this period of crisis.

6. Dominican Republic The Organization of American States team continues its talks with leaders from both sides. It may publicize its proposals Monday in hopes of building up popular support for them.

There is a report that extremists among the rebels are attempting to recruit youths from the countryside for indoctrination and the military training they have been conducting in their Santo Domingo stronghold.

3. Vietnam The North Vietnamese seem to want a war of attrition in the two provinces just south of the Demilitarized Zone.

In a CIA assessment completed this week, we have wrung out the available evidence and we conclude that the enemy is not trying to "liberate" these provinces now. Instead, we feel, the Communists hope to create the illusion of "a war no one can win."

Attacks will be aimed at spreading US forces thin and keeping them under constant pressure without offering the opportunity for a clear-cut allied victory. We believe up to five enemy divisions may now be involved along the zone and in the mountain redoubts to the south.

4. Soviet Union The Soviets are increasing their military presence in Mongolia and they may be about to station a few combat units there. The British ambassador to Ulan Bator says that Russian air force troops are arriving by rail and that many Russian field grade officers have been seen in the capital since March. One Soviet motor pool there has doubled in size since late April.

5. Israel The Israelis continue to threaten the Syrians with retaliation for recent Syrian-supported terrorist incidents. Prime Minister Eshkol has warned publicly that "if there is no other way out," Israel will be forced to take "appropriate means of action" to punish Syria.

New trouble with Jordan is another real possibility. On Monday, the Israelis plan to stage a military parade—perhaps with heavy weapons—in Jerusalem. This would be a clear violation of the armistice of 1949; a nasty incident in the divided city may result.

3. Laos Supplies brought to the North Vietnam–Laos border during late March and April are continuing to filter into Laos toward the Plaine des Jarres. [Still-classified section.] [I]nside Laos report that about 36 trucks a day—the highest rate in recent months—moved west along the route between 6 and 10 May. We still believe that this is a stockpiling operation in anticipation of the rainy season.

4. South Arabia Last week the cabinet in London formally endorsed the decision to unload Britain's South Arabian protectorates next January. The British hope they can give independence to a government with some base of support among the diverse peoples there. This will be difficult and the British will probably accept almost any kind of regime they can get. British troops are to leave as quickly as possible after independence.

A naval force is to be stationed nearby for six months [still-classified material] but there will be no British guarantee against internal subversion—or against a deterioration into political chaos. The whole nasty problem may well end up in the lap of the United Nations.

5. Egypt Nasir is going all out to show that his mutual security pact with Syria is something which the Israelis should take very seriously. Large troop contingents were seen moving through Cairo yesterday and there are other signs of a wide-scale mobilization.

Nasir must be hoping desperately that there will be no need for him to fight the Israelis. He probably feels, however, that his prestige in the Arab world would nose-dive if he stood idly by while Israel mauled Syria again.

6. Egypt—[Still classified.]

7. Dominican Republic Juan Bosch is still in Spain, leading the life of a rather embittered philosopher while his party back home carries on the wars. The latest party move has been to call again for a broad "anti-Trujillo front" to resist the Balaguer government.

So far, the only groups to respond positively to this idea have been extremists of the left. This response has put pressure on party leaders to go ahead with some kind of opposition "front"—even though this would surely produce a further exodus of the more moderate members.

President Balaguer continues on a hard-nosed course as he tries to restore public confidence in the wake of the upsurge of political terrorism. In the process, he is becoming more and more dependent on his conservative and right-wing supporters.

8. Ecuador President Arosemena is faced with a new upsurge of violence. Several people were killed and many wounded late last week before police and troops were able to suppress crowds of workers and students demonstrating their support for striking railwaymen. Further violence is feared and there is talk of more strikes to come.

DAILY BRIEF
27 MAY 1967

1. Arab States–Israel (As of 5:45 AM EDT) No challenge to the blockade appears likely today and there have been no new military developments overnight.

A tanker is due at Eilat about 31 May, but may be diverted as was a sister ship yesterday. A cargo vessel may enter the Gulf on 30 or 31 May.

U Thant may propose that all nations temporarily hold up strategic cargoes (including oil) normally shipped through the Gulf. [Still-classified section.] [A] two-week hiatus on strategic shipping was one of two proposals made by the UN Secretary General during his visit to Cairo. The second proposition was that he send a permanent and personal representative to the Middle East. The Egyptians bought both proposals, [still-classified section].

Moscow is still dodging a definitive position on the blockade. [Still-classified section.] remarked that the Arabs will have a difficult time defending the blockade from the international point of view. [Still-classified section.]

DAILY BRIEF
5 JUNE 1967

1. Arab States Israel Hostilities began early this morning. Both sides report heavy Israel fighting in the air and between armored forces along the Israeli border with Egypt.

Israeli planes raided airfields in Cairo and other areas beginning at about 8:00 AM local time (2:00 AM Washington time).

Cairo has just been informed that at least five of its airfields in Sinai and the Canal area have suddenly become "unserviceable." Israel's war plans had put high priority on quick action against the Egyptian Air Force because of the threat to its own more vulnerable airfields and vital centers.

Reports are still fragmentary, but the signs point to this as an Israeli initiative. Over the weekend it became apparent that Israeli leaders were becoming increasingly convinced that time was running against them. The new Israeli cabinet was meeting late yesterday with Ambassador Harmel present, and reconvened early today.

Cairo radio is calling on Egypt's Arab allies to attack Israel. [Still-classified section.]

2. Libya The big US Wheelus base is becoming more and more exposed to nationalist pressures as the Arab war fever sweeps over this desert kingdom. Cairo is going all out to intensify the pressures, and responsible Libyans are worried; they see no way they can convincingly refute the propaganda that the base is being used to support the Israelis.

The Libyan foreign minister has been in Cairo this weekend, and Wheelus surely must have been discussed during his talk with Nasir.

3. Soviet Union [Still classified.]

4. Nigeria Both sides are preparing for war. Leaders of the breakaway republic in the East have evidence leading them to expect federal troops to attack today. The orderly evacuation of US dependents from the East began yesterday and is to continue today.

The federal government was strengthened over the weekend with the formation of an executive council with civilian representation. The leading political chieftain of the West was included. This has, at least for a time, reduced the danger of Western secession, which would surely have produced serious violence.

LATE ITEMS

Libya The US Embassy in Benghazi flashed word at 4:30 AM EDT that it was being attacked by a large mob. It is burning its papers.

Syria Damascus radio announces that Syrian planes are bombing Israeli cities and that "we have joined the battle."

DAILY BRIEF
6 JUNE 1967

1. Arab States–Israel Cairo may be preparing to launch a campaign urging strikes against US interests in the Arab world. Both Egyptian and Syrian domestic broadcasts this morning called on the "Arab masses" to destroy all US and "imperialist" interests in the "Arab homeland." Last night Cairo radio claimed it had proof of US and British participation in the "aggression."

Demonstrations have now taken place against US embassies and installations all over the Arab world.

Arab oil-producing countries, meeting in Baghdad, say they will stop selling oil to any country which takes part in or supports Israel in the fighting. Baghdad radio said this morning that the pumping of Iraqi oil has been stopped "because of US and UK attitudes."

In the fighting, Israel has gained an early and perhaps overwhelming victory in the air, but the progress of the war on the ground is unclear. If Israeli claims regarding damage to Arab combat aircraft are valid, they have destroyed the entire Jordanian inventory of 21, two thirds of the Syrian inventory of 69, and 250 of some 430 Egyptian planes.

Arab counterclaims of 158 Israeli planes destroyed seem grossly exaggerated, but actual losses to the Israeli force of about 270 aircraft are not known.

Firm information on ground action remains sparse. The Israelis claim they have captured the "outer positions" of Kuntilla in southeastern Sinai and reached the outskirts of al-Arish in northern Sinai.

In Jordan, King Husayn said this morning that Israel is pushing ahead in a "punitive fashion." He ended with a plea that the US intercede.

DAILY BRIEF
7 JUNE 1967

1. Arab States–Israel (As of 5:30 AM EDT) At this point, the shooting continues despite the UN ceasefire resolution. Early this morning Israeli planes were hammering Jordanian positions outside Jerusalem. There also was some firing in the city last night.

The Israelis appear to-hold substantial portions of the' Sinai Peninsula, and Cairo is ordering the Egyptian force at Sharm ash-Shaykh on the Straits of Tiran to withdraw. In fact, there are strong indicat'ions that the Egyptians may be withdrawing most, if not all, of their forces from the Sinai.

Although the Soviets are airlifting in some spare parts for Egyptian tanks and aircraft, there are no indications of any major Soviet military moves. [Still-classified section.]

In last night's Security Council meeting, Federenko demanded withdrawal of forces after a ceasefire, but this performance seems intended to put the best face possible on the retreat. [Still-classified section.]

The US Embassy in Cairo was not set on fire as reported in this morning's *Washington Post.*

DAILY BRIEF
8 JUNE 1967

1. Arab States–Israel (As of 5:00 AM EDT) The UN's ceasefire order is being disregarded. Egypt has officially announced it will not comply, and Nasir has personally so informed most other Arab governments. The Israelis may have broken their ceasefire agreement with Jordan.

Early this morning the Jordanian prime minister told our embassy that Israeli tanks were moving into northwestern Jordan. The ultimate aim of such a movement might be to attack Syria. The embassy also says fighting on the Israeli-Jordanian front picked up during the night. [Still-classified section.]

On the Sinai Peninsula, the Israelis have apparently accomplished most of their military objectives. Yesterday the Israelis approached the Suez Canal so rapidly that they probably cut off the major portion of the retreating Egyptians.

Embassy Cairo believes that public realization of the Arab defeat has generated strong feeling against Nasir, and foreign diplomats in Cairo consider the Egyptians are in a

state of panic over the military debacle. [Still-classified section.] Senior Iraqi officials in New York are said to believe Nasir is desperate and might do almost anything to maintain his position.

Mobs in Dhahran, Saudi Arabia, have damaged US installations, and our consulate in Aleppo has been attacked and burned. As the extent of the defeat sinks into the Arab countries, danger to US citizens still there may increase. Refugees from the fighting in Jordan's West Bank are already streaming into Amman, where they could cause disorder directed at Americans.

LATE ITEM

Arab States–Israel (As of 5:30 AM EDT) The Israelis have just announced (according to the press) that Egyptian armored forces have counterattacked "in force" in an effort to fight their way out of the Sinai Peninsula. This could refer to Egyptian troops trapped in the rapid Israeli advance.

DAILY BRIEF
9 JUNE 1967

1. Arab States–Israel The ceasefire was observed on all fronts during the night. Further Israeli action is still possible against Iraqi forces in Jordan, however, since Baghdad has yet to accept the ceasefire.

The Israeli commander in Sinai reported that his forces were camping on the banks of the Suez Canal and the Red Sea.

Tel Aviv is beginning to discuss the terms it hopes to achieve in a permanent settlement with the Arab states. These include the establishment of an autonomous province of Jordan on the West Bank in which all Arab refugees could hopefully be settled.

The Israelis also intend to insist on the demilitarization of the Gaza strip and the Sinai border, guaranteed access to the Gulf of Aqaba, and an as yet undefined "new status" for a unified Jerusalem. The latter would guarantee people of all religions access to the holy places.

As for the Arab side, attention is now turning to what can be salvaged in post-ceasefire negotiations. Nasir, after earlier proposing an Arab summit as a means of preserving Arab unity, is now proposing the publication of a ten-point joint resolution to be signed by all Arab chiefs of state. The proposed statement trots out all of Nasir's propaganda attacks on the US and other "colonialist forces supporting Israel." On balance, it looks like a rather feeble effort to save face.

Signs are growing that Egypt's defeat has badly damaged Nasir's prestige in the Arab world. He will have trouble getting many other chiefs of state to adhere to his "joint resolution."

2. Arab States Arab resentment against the West continues to threaten US facilities. Libya appears to be a particularly dangerous spot at the moment.

3. Soviet Union The Soviets are finding it hard to conceal their shock over the rapid Egyptian military collapse. A Soviet [still-classified section] could not understand "how our intelligence could have been so wrong." He asked despairingly, "How could we have gotten into such a mess?" Comments from other Soviets, while more restrained, reflect a similar state of mind.

4. Brazil President Costa e Silva is still sidestepping the difficult economic decisions necessary to support the country's vital stabilization program. Anxious to avoid offending any pressure group, he is drifting into policies that could undermine much of the good work begun under Castello Branco.

5. Panama President Robles is trying to keep student agitators off balance until the Canal treaties come up for ratification. This is the reason for unusually harsh sentences handed out to a number of extremist-led students who engaged in a minor ruckus on Tuesday. The bigger, Moscow-oriented student organization at the university is lying low for now, however, and saving its, ammunition for the treaty issue.

LATE ITEM

Arab States–Israel Israeli spokesmen told the press this morning that Egyptian troops had launched an attack on Israeli troops near the Canal, thus violating the ceasefire.

THE PRESIDENT'S DAILY BRIEF
1 APRIL 1968

1. North Vietnam [Still-classified material here] Hanoi reports the Vietnamese Communists are organizing a broad offensive to take place in South Vietnam this summer. [More classified material.] Hanoi expects the offensive to set the stage for a settlement on Communist terms and that the US will accept an "armistice" by early next year. [Classified material] report that a special mobilization of manpower is under way in North Vietnam to provide large numbers of new forces for the South.

* * *

What appear to be eight more infiltration groups were discovered [classified] over the weekend, raising the number of units en route through central North Vietnam in March [classified] More than 17,000 troops could be involved.

2. South Vietnam Vice President Ky, chief of the Joint General Staff Vien, and at least three of the four corps commanders plan to submit their resignations en masse unless Thieu resolves certain doubts and agrees to consult them closely on policy, according to [classified]. These doubts include rumors that Thieu is embarking on wholesale personnel changes which would revive the influence of the southern Dai Viet party at the expense of the military hierarchy.

The commanders are already disturbed by Thieu's recent provincial appointments which they see as a substitution of Thieu's followers for their own protégés or as creating unrest among province chiefs and military officers in general.

3. Panama The Supreme Court will reconvene today to decide on the constitutionality of the Assembly's impeachment of Robles. No matter how the court rules, the situation is likely to deteriorate further.

The people around Arnulfo Arias are now working on more legal moves against the government, and are also keeping pressure on Robles and the National Guard through demonstrations and disorders. If the court invalidates the impeachment, Arias and company are prepared to impeach the court.

Pro-Arias demonstrators plan to be in the streets "to create an atmosphere of tension" while the court is deliberating. Influential families on both sides are becoming more and more convinced that a takeover by the guard is the only solution.

4. Brazil Extremists have taken over the leadership of a major student demonstration planned for today in Rio. Large antigovernment demonstrations already have been held in most key Brazilian cities since the police killed a youth in Rio on Thursday.

The student leaders [classified] plan to focus on the "repressive military dictatorship," but the US will also be a target. There is widespread sympathy for the students' cause.

There is already some evidence of military dissatisfaction with the government's failure to crack down on the students. If students and police clash again, military pressure on the government will probably build quickly.

5. Cyprus Prospects for talks between representatives of the Greek and Turkish communities are better now than at any time since the outbreak of violence in late 1963. Preliminary contacts between the two groups have been aided by the steady decrease in tension since last November. Much distrust remains, however, and no easy solution to the basic problems is in sight.

6. Egypt Nasir, in a speech to the nation on Saturday, outlined a "program of action" to bring about political reform. We doubt that it will amount to much.

[PRESIDENT'S DAILY BRIEF]

The following is the text of an item from the Presidential Daily Brief received by President William J. Clinton on December 4, 1998. Redacted material is indicated in brackets.

SUBJECT: Bin Ladin Preparing to Hijack US Aircraft and Other Attacks

1. Reporting [—] suggests Bin Ladin and his allies are preparing for attacks in the US, including an aircraft hijacking to obtain the release of Shaykh 'Umar 'Abd al-Rahman, Ramzi Yousef, and Muhammad Sadiq 'Awda. One source quoted a senior member of the Gama'at al-Islamiyya (IG) saying that, as of late October, the IG had completed planning for an operation in the US on behalf of Bin Ladin, but that the operation was on hold. A senior Bin Ladin operative from Saudi Arabia was to visit IG counterparts in the US soon thereafter to discuss options—perhaps including an aircraft hijacking.

- IG leader Islambuli in late September was planning to hijack a US airliner during the "next couple of weeks" to free 'Abd al-Rahman and the other prisoners, according to what may be a different source.
- The same source late last month said that Bin Ladin might implement plans to hijack US aircraft before the beginning of Ramadan on 20 December and that two members of the operational team had evaded security checks during a recent trial run at an unidentified New York airport. [—]

2. Some members of the Bin Ladin network have received hijack training, according to various sources, but no group directly tied to Bin Ladin's al-Qa'ida organization has ever carried out an aircraft hijacking. Bin Ladin could be weighing other types of operations against US aircraft. According to [—] the IG in October obtained SA-7 missiles

and intended to move them from Yemen into Saudi Arabia to shoot down an Egyptian plane or, if unsuccessful, a US military or civilian aircraft.

- A [—] in October told us that unspecified "extremist elements" in Yemen had acquired SA-7s. [—]

3. [—] indicate the Bin Ladin organization or its allies are moving closer to implementing anti-US attacks at unspecified locations, but we do not know whether they are related to attacks on aircraft. A Bin Ladin associate in Sudan late last month told a colleague in Kandahar that he had shipped a group of containers to Afghanistan. Bin Ladin associates also talked about the movement of containers to Afghanistan before the East Africa bombings.

- In other [—] Bin Ladin associates last month discussed picking up a package in Malaysia. One told his colleague in Malaysia that "they" were in the "ninth month [of pregnancy]."
- An alleged Bin Ladin supporter in Yemen late last month remarked to his mother that he planned to work in "commerce" from abroad and said his impending "marriage," which would take place soon, would be a "surprise." "Commerce" and "marriage" often are codewords for terrorist attacks. [—]

FOR THE PRESIDENT ONLY
6 AUGUST 2001
BIN LADIN DETERMINED TO STRIKE IN US

Clandestine, foreign government, and media reports indicate Bin Ladin since 1997 has *wanted to conduct terrorist attacks in the US.* Bin Ladin implied in US television interviews in 1997 and 1998 that his followers would follow the example of World Trade Center bomber Ramzi Yousef and "bring the lighting to America."

After US missile strikes on his base in Afghanistan in 1998, Bin Ladin told followers he wanted to retaliate in Washington, according to a [—] service.

An Egyptian Islamic Jihad (EIJ) operative told an [—] service at the same time that Bin Ladin was planning to exploit the operative's access to the US to mount a terrorist strike.

The millennium plotting in Canada in 1999 may have been part of Bin Ladin's first serious attempt to implement a terrorist strike in the US. Convicted plotter Ahmed Ressam has told the FBI that he conceived the idea to attack Los Angeles International Airport himself, but that Bin Ladin lieutenant Abu Zubaydah encouraged him and helped facilitate the operation. Ressam also said that in 1998 Abu Zubaydah was planning his own US attack.

Ressam says Bin Ladin was aware of the Los Angeles operation.

Although Bin Ladin has not succeeded, his attacks against the US Embassies in Kenya and Tanzania in 1998 demonstrate that he prepares operations years in advance

and is not deterred by setbacks. Bin Ladin associates surveilled our Embassies in Nairobi and Dar es Salaam as early as 1993, and some members of the Nairobi cell planning the bombings were arrested and deported in 1997.

AI-Qa'ida members—including some who are US citizens—have resided in or traveled to the US for years, and the group apparently maintains a support structure that could aid attacks. Two al-Qa'ida members found guilty in the conspiracy to bomb our Embassies in East Africa were US citizens, and a senior EIJ member lived in California in the mid-1990s.

A clandestine source said in 1998 that a Bin Ladin cell in New York was recruiting Muslim-American youth for attacks.

We have not been able to corroborate some of the more sensational threat reporting, such as that from a [—] service in 1998 saying that Bin Ladin wanted to hijack a US aircraft to gain the release of "Blind Shaykh" 'Umar 'Abd al-Rahman and other US-held extremists.

Nevertheless, FBI information since that time indicates patterns of suspicious activity in this country consistent with preparations for hijackings or other types of attacks, including recent surveillance of federal buildings in New York.

The FBI is conducting approximately 70 full field investigations throughout the US that it considers Bin Ladin-related. CIA and the FBI are investigating a call to our Embassy in the UAE in May saying that a group of Bin Ladin supporters was in the US planning attacks with explosives.

APPENDIX G

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE CRITIQUE OF HUMINT, 2004

AREAS OF SPECIAL INTEREST

In the following several pages, the Committee highlights areas of concern that it believes must be addressed with a high priority by the Director of Central Intelligence, (DCI) as the leader of the Intelligence Community, if intelligence sufficient to protect our national security is to be obtained and provided to policy makers. The Committee places particular emphasis on issues that impact the Intelligence Community as a whole or that involve several various programs.

GLOBAL HUMAN INTELLIGENCE COLLECTION

All is not well in the world of clandestine human intelligence collection (HUMINT). The DCI himself has stated that five more years will be needed to build a viable HUMINT capability. The Committee, in the strongest possible terms, asserts that the Directorate of Operations (DO) needs fixing. For too long the CIA has been ignoring its core mission activities. There is a dysfunctional denial of any need for corrective action. The CIA must collect against all types of targets needed to gain the insights into plans and intentions of our adversaries, be they terrorist, political, economic, military, in nature. Countering the threat from terrorism is, of course, and should be, at the top of CIA's list of collection priorities, but the Central Intelligence Agency must continue to be much more than just the "Central Counterterrorism Agency" if America is to be truly secure, prosperous, and free.

The Committee has placed in the classified annex of this intelligence authorization its comprehensive analysis of what specifically is not right with the way the Directorate of

---

Source: Excerpt from "Intelligence Authorization Act for Fiscal Year 2005," *Report 108-558*, Permanent Select Committee on Intelligence (the Goss Committee), U.S. House of Representatives, 108th Cong., 2d Sess. (June 21, 2004), pp. 23–27.

Operations is being and has been managed. The Committee also assesses that the consequences of continued CIA mismanagement of the HUMINT mission are significant. Replete throughout this analysis, which includes specific recommendations for corrective action, are footnoted references to similar criticisms made by this Committee in the classified annexes of past intelligence authorization bills stretching back well before the 9/11 terrorist attacks. So, this is not new territory for the Committee. CIA has officially registered its strong objection to the Committee's exhaustively researched conclusions, which were reached over the course of years of close oversight and informed by hundreds of meetings and continuous dialogue with experienced CIA field operatives and Headquarters officials. That none of it could be made unclassified is unfortunate.

The Committee respects the authority of the DCI to make classification decisions and will, of course, abide by his ruling in this matter. After years of trying to convince, suggest, urge, entice, cajole, and pressure CIA to make wide-reaching changes to the way it conducts its HUMINT mission, however, CIA, in the Committee's view, continues down a road leading over a proverbial cliff. The damage to the HUMINT mission through its misallocation and redirection of resources, poor prioritization of objectives, micromanagement of field operations, and a continued political aversion to operational risk is, in the Committee's judgment, significant and could likely be long-lasting. Immediate and far-reaching changes can still reverse some of the worst factors eroding its capabilities, however. If the CIA continues to ignore the experience of many of its best, brightest, and most experienced officers, and continues to equate criticism from within and without—especially from its oversight committees—as commentary unworthy even of consideration, no matter how constructive, informed, and well-meaning that criticism may be, they do so at their peril. The DO will become nothing more than a stilted bureaucracy incapable of even the slightest bit of success. The nimble, flexible, core-mission oriented enterprise the DO once was, is becoming just a fleeting memory. With each passing day, it becomes harder to resurrect. The Committee highlights, with concern, the fact that it only took a year or two in the mid-1990's to decimate the capabilities of the CIA, that we are now in the 8th year of rebuild, and still we are more than 5 years away from being healthy. This is tragic. It should never happen again.

The Committee believes that the DO's difficulties are manifest in the discussion on Iraq's WMD. The analysts have taken a significant amount of criticism on the issue. It is imperative to point out, however, that the analysts do not collect the information they analyze. They simply take what is available and reach educated assessments. It is incumbent on the DO and other areas of the IC collection community to gather the information that will present a more complete picture. There was an insufficiency of the right amount of information available on this topic for the analysts. The U.S. cannot afford to be in such a position.

THE STATE OF THE CIA'S DIRECTORATE OF INTELLIGENCE (DI)

In the aftermath of the terrorist attacks on the United States on September 11, 2001, the CIA's Directorate of Intelligence has experienced dramatic personnel shifts and a rapid increase in the demand for both its analysts and work product. The DI, much like the CIA's clandestine arm, the Directorate of Operations, suffered from disinvestments resulting from the so-called "peace dividend" of the 1990's. It was not until the World Trade Center and Pentagon were struck that senior DI management began to realize just how desperate the need is for an expanded and experienced analytic cadre.

DI analysts have earned a reputation in the Intelligence Community for being highly educated, well trained, motivated, and capable of handling demanding and fast moving assignments. As a result, with the expansion of the terrorist mission, DI analysts are in demand across the Intelligence Community, and in line with the CIA's "can-do" attitude has committed significant numbers of DI analysts to other organizations and posts. The CIA's analytic cadre, much like its covert counterpart in the DO, toil quietly, without significant praise, seldom ever to tell of success publicly, but sharply criticized for the least inaccuracy. The Committee notes the hard-working and dedicated rank-and-file professionals that provide the link between collection and truth and add value to raw data for policymakers.

The Committee notes four developments that, if not adequately addressed in the near-term, will work together to seriously undermine and degrade the relevance of the DI and its critically important products at a time when they are needed most by consumers. The first factor—the unsustainable surges in DI personnel to cover crisis issues without adequate back-filling—may be the easiest of the four problems to address. Aggressive new hiring is helping to mitigate this problem, but in the interim, overall DI expertise is declining, as new analysts need substantial training and on-the-job learning of their accounts. While there may be a strong temptation to surge these analysts to meet new crisis needs, it is important that this not be done prematurely or so haphazardly that it creates more problems than it seeks to solve. DI analysts must be allowed to develop true expertise. The DI must not be permitted to become an organization of generalists. Longer assignments on specific countries, regions, or issues—once discouraged by DI management concerned about analytic "clientitis"—should be strongly encouraged. This is, in the Committee's view, a major way to reverse permanently the trend towards widening global analytic gaps. Analytic depth can be more about skills than about numbers of bodies.

The second major DI problem area concerns the culture of analytic risk aversion, begun long before 9/11, but fostered through the continued perception on the part of the rank-and-file that senior DI managers do not want risk taking—however calculated, caveated, and warranted—and that they will not stand by an analyst who has made the wrong prediction. With some exceptions, the DI has become more focused on coordinated judgments that are often so caveated that they are of little use to consumers who are searching for some form of clarity in the very gray world of finished intelligence reporting. While clarity will not always be possible, analysts should be encouraged to be more forward leaning and to push the analytic envelope whenever possible, lest consumers turn more and more—as they have in recent years—to uncorroborated single-source HUMINT or SIGINT reports to inform their decisions. Creating an environment of some stability for analysts to develop adequate expertise will be an essential part of breaking the DI's risk averse culture, lest risk-taking become a reckless rather than calculated process.

The Committee recognizes that the DI is suffering from the difficult combination of vastly increasing requirements and too few bodies to service them. Strong DI leadership, however, with a demonstrated commitment to calculated risk-taking and to the true expertise building that must come with it, would begin to bridge the gap between where DI personnel numbers are now and the time when adequate help arrives. With the CIA's analysis on Iraq being widely criticized, DI leaders simply cannot afford to sit on their heels. If analysts decided to give up on risk-taking entirely, the national security interests of the country will suffer. This cannot be permitted to happen.

The third major problem area was also clearly evident to the Committee as a problem in the years before 9/11 and appeared in the form of criticial classified report language in

past intelligence authorizations. This is the continuing overemphasis by senior DI managers on current intelligence reporting instead of on the longer-term, predictive, strategic intelligence forecasting that was once the strength of the DI and the staple of the DI's avid consumer base. The explosion of all form of open-source reporting, combined with technology for transmitting news across the globe in near-real time makes it nearly impossible for DI analysts to keep up. Instead of "chasing CNN," as the Committee has observed in the past, the DI should be devoting much more of its resources to doing the kind of all-source, in-depth analysis that cannot, and is not, being done elsewhere in government or through media outlets. The DI will always have to leave some capability in place to make sure that its judgments about overnight developments in the world's hot spots are rapidly provided to consumers each day via tried and tested means, such as daily publications, spot reports, and briefings, for example. But, analysts have complained for years, and the Committee has heard the message loud and clear, that the preference of senior DI managers for current intelligence and opportunities to brief such product to high-level consumers far outstripped the DI's capacity to be useful. More importantly, such DI priorities damaged the DI's base of expertise by squandering scarce analytic resources that could be put to better use helping the more sophisticated line-consumers understand better what was behind the facade of the daily or hourly news reports. The crisis atmosphere post-9/11 has indeed generated more interest in rapid analytic judgments to address fast-moving situations, but the DI needs to play to its strengths and fill a badly needed function of giving the consumer a much higher degree of education than the "sound-bite" analysis currently being emphasized. These are the types of priorities to be set by the DI's top manager. The Committee continues to disagree with the rationale for the continuing trend towards current intelligence at the expense of nearly every other form of the discipline.

Finally, the Committee remains concerned that senior DI managers still do not have the ability to drive collection priorities, despite past Committee exhortations about the urgency of fixing this problem, and the CIA's own stated goals. A number of analytic judgments on Iraq have so far been found to be inconsistent with the facts on the ground. While intelligence analysis seldom, if ever, provides a 100 percent accurate picture, deficiencies were largely the result of years of inadequate or insufficient HUMINT collection, and extensive and ingrained denial and deception tactics that defeated technical collection efforts. Analysts had little actual ground truth with which to work. The Committee now finds the DO overly focused on a few priority targets, leaving analysts once again reliant on the media and other mostly open or insufficiently validated sources of information with which to make its key judgments. Given the recent performance on Iraq, the Committee believes that senior DI management should play a stronger role in determining collection priorities and advocating the need for global coverage.

APPENDIX H

SENATE SELECT COMMITTEE ON INTELLIGENCE REPORT ON IRAQI WMD INTELLIGENCE, 2004

I. INTRODUCTION

(U) In June 2003, the Senate Select Committee on Intelligence began a formal review of U.S. intelligence into the existence of Iraq's weapons of mass destruction (WMD) programs, Iraq's ties to terrorist groups, Saddam Hussein's threat to stability and security in the region, and his violations of human rights including the actual use of weapons of mass destruction against his own people, as a part of the Committee's continuing oversight of the intelligence activities of the United States.

(U) Committee staff had, for the previous several months, already been examining aspects of intelligence activities regarding Iraq, including the Intelligence Community's (IC's) intelligence support to the United Nations Monitoring, Verification, and Inspection Commission (UNMOVIC) weapons inspections in Iraq and the IC's analysis and collection of reporting related to the alleged Niger-Iraq uranium deal. On June 20, 2003, however, Senator Pat Roberts, Chairman, and Senator John D. Rockefeller IV, Vice Chairman, of the Senate Select Committee on Intelligence released a press statement announcing their joint commitment to continue the Committee's thorough review of U.S. intelligence. Chairman Roberts and Vice Chairman Rockefeller said the Committee would examine:

- the quantity and quality of U.S. intelligence on Iraqi weapons of mass destruction programs, ties to terrorist groups, Saddam Hussein's threat to stability and security in the region, and his repression of his own people;
- the objectivity, reasonableness, independence, and accuracy of the judgments reached by the Intelligence Community;

Source: Excerpt from *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq* (the Roberts Report), Senate Select Committee on Intelligence (the Roberts Committee), U.S. Senate, 108th Cong., 2d Sess. (July 7, 2004), pp. 1–35.

- whether those judgments were properly disseminated to policymakers in the executive branch and Congress;
- whether any influence was brought to bear on anyone to shape their analysis to support policy objectives; and
- other issues we mutually identify in the course of the Committee's review.

With the exception of the question of accuracy, all of the foregoing are addressed in this report.

(U) On February 12, 2004, the Committee unanimously agreed to refine the terms of reference of the Committee's inquiry. In addition to the matters set forth in the joint release of the Chairman and Vice Chairman on June 20, 2003, the Committee agreed to examine additional issues in two phases. Issues annotated as phase one have been addressed in this report. Issues annotated as phase two are currently under review by the Committee. The additional issues are:

- the collection of intelligence on Iraq from the end of the Gulf War to the commencement of Operation Iraqi Freedom (phase I);
- whether public statements, reports, and testimony regarding Iraq by U.S. Government officials made between the Gulf War period and the commencement of Operation Iraqi Freedom were substantiated by intelligence information (phase II);
- the postwar findings about Iraq's weapons of mass destruction and weapons programs and links to terrorism and how they compare with prewar assessments (phase II);
- prewar intelligence assessments about postwar Iraq (phase II);
- any intelligence activities relating to Iraq conducted by the Policy Counterterrorism Evaluation Group (PCTEG) and the Office of Special Plans within the Office of the Under Secretary of Defense for Policy (phase I and II); and
- the use by the Intelligence Community of information provided by the Iraqi National Congress (INC) (phase I and II).

(U) In early June 2003, the IC provided the Committee with nineteen volumes (approximately 15,000 pages) of intelligence assessments and source reporting underlying the IC's assessments of Iraq's WMD programs, ties to terrorist groups, threat to stability and security in the region, and repression of its own people. Committee staff began immediately to read and analyze every report provided to determine how intelligence analysts reached their conclusions and whether any assessments were not supported by the intelligence provided to the Committee. In late August and early September 2003, Committee staff requested additional intelligence to support IC assessments which Committee staff had judged were not supported by the intelligence that had been previously provided.

(U) The Committee began to receive this additional supporting intelligence in October 2003. In late October 2003, Committee staff requested that the IC provide any intelligence, which had not already been provided, that contradicted the IC's analyses regarding Iraq. For example, Committee staff requested intelligence that showed Iraq had not reconstituted its nuclear program, had not renewed production of chemical agents, and had abandoned an offensive biological weapons program. In early November 2003, the IC wrote to the Committee that it was working to provide the contradictory intelligence requested by Committee staff. In the same letter, the IC said it had uncovered an additional

six volumes of intelligence material that supported the IC's assessments on Iraq's WMD programs. These materials were also reviewed by Committee staff. The IC provided the contradictory intelligence information in late November. During the twelve months of the Committee's review, Committee staff submitted almost 100 requests for supplemental intelligence information, received over 30,000 pages of documents in response to those requests, and reviewed and analyzed each document provided. The Committee's request to review Presidential Daily Briefs (PDBs) relevant only to Iraq's weapons of mass destruction capabilities and links to terrorists was denied by the White House. Without examining these documents, the Committee is unable to determine fully whether Intelligence Community judgments were properly disseminated to policymakers in the executive branch, one of the tasks outlined for review.

(U) Committee staff interviewed more than 200 individuals including intelligence analysts and senior officials with the Central Intelligence Agency (CIA), Defense Intelligence Agency, Department of Defense, Department of Energy, Department of State, National Ground Intelligence Center, the Air Force, and the Federal Bureau of Investigation. Staff also interviewed former intelligence analysts, National Intelligence Officers, operations officers, collection managers, signals intelligence collectors, imagery analysts, nuclear experts with the International Atomic Energy Agency, Ambassadors, former United Nations inspectors, Department of Defense weapons experts, State Department officials, and National Security Council staff members.

(U) The Committee held four preliminary hearings on aspects of U.S. intelligence on Iraq: the Iraq-Niger connection, the CIA and State Department Inspectors General report on the review of the Iraq-Niger issue, the history and continuity of weapons of mass destruction assessments pertaining to Iraq, and Iraq prewar intelligence.

(U) These efforts have enabled the Committee to develop a full understanding of the quantity and quality of intelligence reporting on Iraq's WMD programs, Iraq's ties to terrorist groups, Saddam Hussein's threat to stability and security in the region, and his violations of human rights including the actual use of weapons of mass destruction against his own people. The Committee has also gained an understanding of how intelligence analysts throughout the IC used that intelligence to develop their assessments on these issues, how those assessments were disseminated to policymakers, whether those assessments were reasonable, objective, independent of political consideration, and whether any influence was brought to bear to shape their analysis to support policy objectives.

A. UNDERSTANDING INTELLIGENCE ANALYSIS

(U) Over a period of one year, Committee staff, many of whom are former intelligence analysts, reviewed over a decade of Intelligence Community (IC) assessments and the intelligence that underlay them. In all cases our staff endeavored, to the greatest extent possible, to disregard post-war discoveries concerning Iraq until after completing the analysis of the prewar intelligence material in order to replicate the same analytical environment IC analysts experienced prior to the war. The Committee's review surfaced strengths and weaknesses throughout the intelligence process. These are identified in the Report's findings and conclusions.

(U) Intelligence analysis is not a perfect science and we should not expect perfection from our IC analysts. It is entirely possible for an analyst to perform meticulous and skillful analysis and be completely wrong. Likewise, it is also possible to perform careless

and unskilled analysis and be completely right. While intelligence collection is not an analytical function, it is the foundation upon which all good analysis is built. Problems with collection priorities and management will be discussed in detail throughout the report.

(U) The Committee, therefore, believes that it is important to understand the role of analysts and how they learn and apply their craft. With that background, the Committee hopes the reader can fully appreciate the content of this report.

1. Developing Professional Intelligence Analysts

(U) In order to give context to the Committee's review of the Intelligence Community's (IC) prewar analyses, Committee staff spoke with senior CIA officers at the Sherman Kent School for Intelligence Analysis at the CIA. The CIA relies on the Kent School to teach new analysts the trade craft of analysis. Committee staff members also drew on their own experiences working in the IC's analytic community.

(U) Kent School officials provided a briefing, slides, and a copy of the school's brochure to explain the school's approach and how analytic trade craft is presented to new CIA analysts. The training also address how the Directorate of Intelligence (DI) views the analytic process and the DI's structure.

(U) The CIA's Directorate of Intelligence requires its new analysts to complete a training program called the Career Analyst Program, or CAP. The CAP includes eleven weeks of classroom instruction and a five week interim assignment. The participants receive two weeks of training on analysis, three weeks on DI writing and one week each on briefing, teamwork, and the business of intelligence. (These are the core analytic trade craft areas.) The CAP also devotes time to task-force exercises and visits to U.S. military commands and other agencies to help the students develop a broader perspective on the role of intelligence analysis in policymaking. For the interim assignment, analysts consult with their "home offices" to choose an assignment that is relevant to the account they will cover as a DI analyst. They can work in other intelligence agencies, a policy office or in a law enforcement agency for their interim assignment.

(U) According to the school's brochure, "The CAP emphasizes the Directorate's goal: to produce analysis that is rigorous, well-reasoned, and appropriately caveated. The analytic thinking courses' focus on questioning key assumptions and considering possible explanations and outcomes. Analysts learn to be aware of psychological, cultural, and informational factors that affect their analytic judgments." Kent School officials stated that this training involves a very hands-on approach and many small exercises that help the analysts learn by doing. Instructors give the students a number of short classroom assignments, many of which are done in groups. Students receive extensive feedback from the instructors.

(U) The same is true for the development of the analysts' writing skills. The long brochure states, "DI writing style emphasizes the bottom line up front, precise and concise language, and a clear articulation of our judgments and our confidence in them." The analysts practice writing each of the types of products that the DI produces including situation reports and short and long papers. They also participate in a final four-day course on writing for the President and senior policymakers. The Kent School officials stated that many of these assignments use case studies, such as the attack on Pearl Harbor, the Cuban Missile Crisis, the bombing of Khobar Towers, the break-up of Yugoslavia and the September 11 attacks.

(U) Kent School officials outlined the key analytic goals as:

- providing timely, credible, and relevant intelligence analysis for the consumer;
- warning and identifying opportunities;
- maintaining analytic integrity and objectivity; and
- using all source intelligence.

They also described the analytic process as 1) dealing with facts and assertions, 2) testing assumptions and logic, 3) developing findings, 4) interpreting information, 5) developing scenarios (to include both high probability/low impact and low probability/high impact), 6) determining indicators, and 7) discussing options to determine opportunities, identifying vulnerabilities and revealing potential outcomes.

(U) By using case studies and providing the CAP participants with the intelligence cables used by analysts to build their assessments, the instructors are able to help the new analysts develop their ability to weigh information and become accustomed to the format of the reporting and source descriptions. They also learn to task collectors, structure data for presentations, and recognize indicators of activities. They also learn to recognize the strengths and weaknesses of the various "INTs"—human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), and measurement and signature intelligence (MASINT).

(U) The Kent School also incorporates a module which alerts new analysts to the pitfalls of assumptions and biases in their own analysis and in the work of others. Recognizing one's own bias is extremely difficult, however. Therefore, it is critical to develop a workforce of analysts that are comfortable questioning each other. While it is stressed in the initial training provided by the CAP, it appears to be the lesson that analysts neglect first.

(U) In her February 11, 2004 address to the Directorate of Intelligence, the Deputy Director for Intelligence (DDI) stated:

> I want to focus on the danger of inherited assumptions. That may be the single most important aspect of our trade craft that needs to be examined. That is something I speak about to every new CAP class: How do we ensure that we are not passing along assumptions that haven't been sufficiently questioned or examined?

2. An Analyst's Daily Taskings

(U) In terms of day-to-day work, intelligence analysts review raw reporting, draft assessments, and disseminate those assessments to policy makers. Each written assessment may be drafted by one or several analysts who have reviewed raw reporting over a period of time. Intelligence collected by the CIA, Defense Intelligence Agency (DIA), National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA) and in some cases, State Department diplomatic reporting, is reviewed daily by intelligence analysts using computer software that searches the various agencies' databases and produces a daily electronic read file for each analyst that is specific to their area of responsibility. In many instances, analysts from regional and functional offices, which cover issues that span across regions, such as terrorism, drug trafficking, and humanitarian issues, will read the same material and draw conclusions relative to their interests and responsibilities.

(U) Each IC agency that has an all-source analysis capability or responsibility will have one or more analysts reviewing intelligence reporting on the same issues. In an ideal

situation, these analysts will be in regular contact over secure communications to discuss new information, to share ideas and to brainstorm about how the information can be presented to policymakers to best satisfy their requirements, however, this exchange does not always occur. The analysts are responsible for sifting through large amounts of information and drawing connections or reaching conclusions about the implications of the information at their disposal. Depending on the product, the analysis may be coordinated with other IC members, but in many instances, each agency produces its own finished products which are subject to review and editing by its own internal management.

3. The Finished Product

(U) Analysts create their products for intelligence consumers, including policy makers and warfighters, to name two of many. While DIA products are generally intended for the Secretary of Defense, CIA products for the White House, and the State Department's Bureau Intelligence & Research products for the Secretary of State, most products are available to policy makers at each of these agencies regardless of the author's organization. The vast majority of intelligence products are available to the Congress as well.

(U) It is important to note that in many cases the manager responsible for approving the final product may not, and often does not, review the raw intelligence upon which the assessment is based. Kent School officials who have worked as branch chiefs or division managers stated, however, that products are reviewed more carefully when the drafter is a relatively new analyst. When the drafter is a more senior, well-established analyst, the product will often be edited, but not substantively reviewed before it goes up the chain to the policymaker. If the intelligence product was not coordinated with other intelligence agencies, it is entirely possible that one analyst's views may be presented to high-level officials including the President of the United States without having been reviewed by other analysts with the same depth of knowledge. This is a dynamic we found on a number of occasions in the course of this review.

B. WEAPONS OF MASS DESTRUCTION CAPABILITIES

(U) The Weapons of Mass Destruction (WMD) related sections of the report recount the Committee's efforts to evaluate the quantity and quality of the intelligence underlying prewar assessments. Each section contains its own set of conclusions. There is also a separate section on the issue of objectivity which addresses whether analysts were pressured to reach specific conclusions to support a particular policy objective. This report does not address the question of accuracy regarding WMD. When the Iraq Survey Group (ISG) completes its work in Iraq, we will then be able to evaluate to the maximum extent possible the accuracy of the IC's judgments prior to the war.

(U) The Committee focused its evaluation of the Intelligence Community's WMD analysis primarily on the October 2002 National Intelligence Estimate (NIE): *Iraq's Continuing Programs for Weapons of Mass Destruction.* This document was selected for several reasons:

- First, according to the National Intelligence Council (NIC) and the Director of Central Intelligence (DCI), National Intelligence Estimates (NIE) are the IC's most authoritative written judgments concerning national security issues. The process by which the IC produces NIEs—including the one on Iraqi WMD—has been honed

over nearly 30 years. According to the Central Intelligence Agency's (CIA) webpage, it is designed to provide policymakers in both the executive and legislative branches with the "best, unvarnished, and unbiased information—regardless of whether analytic judgments conform to U.S. policy."

- Second, the 2002 NIE addressed all of Iraq's WMD programs and was a coordinated community judgment in which all agency views were represented and dissenting opinions were noted.
- Third, the 2002 NIE was comprehensive, encompassing more than ten years of source reporting and analysis. The intelligence documentation provided to the Committee to support the assessments in the 2002 NIE also included the documents which were the basis for the previous decade of analytical products on Iraq's WMD programs.
- Fourth, the 2002 NIE presented some new IC assessments, some of which shifted in significant ways from previous judgments regarding Iraq's WMD programs.
- Finally, the 2002 NIE was requested by Senate Select Committee on Intelligence (SSCI) Members so that policymakers could benefit from the IC's coordinated judgment on Iraq's WMD programs while they debated authorizing military action against Iraq.

(U) Since June 2003, Committee staff has worked through a decade of intelligence assessments on Iraqi WMD programs and the intelligence source reporting used by IC analysts to make those assessments—over 20,000 pages of documents. Committee staff interviewed over 160 people, including intelligence analysts from every agency involved in preparing WMD assessments on Iraq, ambassadors, operations officers, collection managers, nuclear experts with the International Atomic Energy Agency (IAEA), former United Nations (UN) inspectors, Department of Defense (DoD) weapons experts, State Department officials, and National Security Council (NSC) staff members.

(U) These efforts have enabled Committee staff to develop a full understanding of the body of intelligence on Iraq's WMD capabilities and an understanding of how intelligence analysts throughout the IC used that body of intelligence reporting to develop their assessments, particularly those in the 2002 NIE on *Iraq's Continuing Programs for Weapons of Mass Destruction.*

1. What is an NIE?

(U) A National Intelligence Estimate is the IC's most authoritative written judgment concerning a specific national security issue. The Estimates are intended to provide policymakers in both the executive and legislative branches with the best, unvarnished, and unbiased information—regardless of whether analytic judgments conform to any particular policy objective.

(U) A 2003 NIC paper on the NIE process stated that an NIE is "...the most authoritative written means by which the Director of Central Intelligence conveys to the President and other senior leaders the judgments of the entire Intelligence Community regarding national security issues." Sherman Kent,[1] a former Chairman of the Board of

[1] *Sherman Kent and the Board of National Estimates: Collected Essays,* (Http://www.odci.gov/csi/books/shermankent/inst.html). From 1952 to 1967, Sherman Kent was the Chairman of the Board of National Estimates, which would later become the National Intelligence Council.

National Estimates, described the purpose and importance of NIEs in an essay in 1976, which noted that the NIE

> . . . was and is the Director's estimate, and its findings are his. Although many experts from perhaps all intelligence components of the community participated in the production of the papers in the NIE series, and although the intelligence chiefs themselves formally passed on the final text, they could not bend its findings to suit their own judgments contrary to the will of the DCI. They could try to win him to their sides by full and free discussions, but they could not outvote him and force him to join them, nor could they make him dissent from them . . . they could of their own accord concur with his findings or, not being able to, they could dissent and make their alternative views known in footnotes to his text.

(U) NIEs and the formal process by which they are produced, were established in the 1950s. An NIE can be requested by a variety of individuals, including members of the executive branch, members of Congress, and military commanders. After an NIE has been requested and authorized, the next step is the preparation of a document which has come to be called the Terms of Reference (TOR). According to a 1994 NIC paper describing NIE drafting guidelines, the TOR is an outline of the "issues and key questions to be covered in the Estimate." Sherman Kent describes the TOR as a "statement of precisely what was wanted."

(U) An officer of the NIC, typically the National Intelligence Officer (NIO) with responsibility for the substantive issue being examined in the NIE, is given responsibility for managing the NIE from its initial drafting, through the coordination process with the national intelligence agencies, to final approval. The officer presiding over the drafting of the NIE can draw on the staff of the NIC as well as the national intelligence agencies to write the draft.

(U) The 1994 NIE drafting guidelines state that an NIE can be drafted by an IC analyst, a member of the NIC staff, a deputy NIO, or an outside expert. After the draft has been reviewed within the NIC staff, it is then sent to the national intelligence agencies where each agency's appropriate subject matter experts review the draft and prepare their comments. Agency comments are then carried forward to the first interagency coordination session. At this and any successive coordination sessions, the goal is to produce a draft that, without unnecessary hedging or ambiguity, reflects the collective judgment of the IC. In the event any of the agency representatives find a part of the NIE with which they do not concur, they are free to argue their case before their colleagues in order to sway them. If they fail to convince their colleagues, they are free to draft a dissenting footnote. Once the agency representatives arrive at a consensus paper, with or without footnotes, this final draft is usually submitted to IC peers and to a panel of IC experts for their review. A summary of the outside experts' views is included in the NIE. The NIC front office reviews the final draft prior to forwarding it to the National Foreign Intelligence Board (NFIB) principals for their approval. The NFIB is composed of senior representatives of the IC organizations involved in the collection, processing and analysis of intelligence[2] and is

[2] The members of the NFIB are the DCI; Deputy Director of Central Intelligence (DDCI); Associate Director of Central Intelligence for Military Support; Assistant Secretary for Intelligence and Research (INR), Department of State; Deputy Director for Intelligence (DDI), Central Intelligence Agency (CIA); Director, Defense Intelligence Agency (DIA); Director, National Security Agency (NSA); Director, National Geospatial-Intelligence Agency (NGA); Executive Assistant Director, Federal Bureau of Investigation (FBI); Director, Office of Intelligence, Department of Energy (DOE); Special Assistant to the Secretary of the Treasury; Chairman, National Intelligence Council.

chaired by the DCI. The senior representatives of the military intelligence services may also attend as members of the NFIB when matters under their purview are considered and may attend other NFIB sessions as observers. The NFIB typically approves the NIE the same day it is presented.

(U) The 1994 NIE drafting guidelines described three rough time frames for the production of an NIE: a "fast track" of two to three weeks, a "normal track" of four to eight weeks, and a "long track" of two months or more. The Vice Chairman of the NIC told Committee staff that an NIE prepared within 60 days would be considered very fast, and that typically NIE's take three to six months. Sherman Kent noted in his essay that prior to 1976, NIE's had historically taken up to six to eight months to produce, but under conditions of urgency the time line has been considerably shortened. For example, during the Suez crisis of 1956, the Soviets sent a threatening note to Britain and France, who, along with the Israelis, had begun an attack on Egypt. The acting DCI convened the heads of the national intelligence agencies to develop an NIE to provide the IC's appraisal of Soviet intentions. There were no TORs and a draft was produced in about 30 minutes. The draft was immediately presented to the heads of the IC, who discussed and cleared the NIE within a few hours. The NIOs told Committee staff that ideally they would like about three months to produce an NIE.

2. The 2002 NIE on Iraq's Continuing Programs for Weapons of Mass Destruction

(U) In an unclassified letter dated September 9, 2002, Senator Richard Durbin, a member of the SSCI, wrote to the DCI expressing concern that the IC had not drafted an NIE on the status of Iraq's WMD program, and requested that the DCI "direct the production" of such an NIE—expressing the belief that "policymakers in both the executive branch and the Congress will benefit from the production of a coordinated, consensus document produced by all relevant components of the Intelligence Community" on this topic. Senator Durbin also requested that the DCI "produce an unclassified summary of this NIE" so "the American public can better understand this important issue."

(U) On September 10, 2002, Senator Bob Graham, then SSCI Chairman, sent a second letter to the DCI requesting the production of an NIE "on the status of Iraq's programs to develop weapons of mass destruction and delivery systems, the status of the Iraqi military forces, including their readiness and willingness to fight, the effects a U.S.-led attack on Iraq would have on its neighbors, and Saddam Hussein's likely response to a U.S. military campaign designed to effect regime change in Iraq."

(U) On September 13, 2002, Senator Diane Feinstein, a member of the SSCI, wrote to President Bush to request his assistance in ensuring that the DCI prepare, on an immediate basis, an NIE "assessing the nature, magnitude and immediacy of the threat posed to the United States by Iraq." Senator Feinstein added, "there has not been a formal rigorous Intelligence Community assessment, such as a National Intelligence Estimate, addressing the issues relating to Iraq, and I deeply believe that such an estimate is vital to Congressional decision making, and most specifically, any resolution which may come before the Senate."

(U) On September 17, 2002, Senator Carl Levin, a member of the SSCI and then Chairman of the Senate Armed Services Committee, wrote to the DCI stating that it was "imperative" for the IC to prepare an NIE on Iraq "including the central question of the current state of Iraq's weapons of mass destruction programs." Senator Levin asked that

the NIE address a number of issues including Iraq's WMD holdings, development facilities, acquisition activities, denial and deception activities, deployment, doctrine for employment, means of delivery, the likelihood that Saddam Hussein would use WMD against the U.S., our allies, or our interests, the likelihood that Iraq would comply with UN resolutions; and Iraq's terrorist activities.

(U) By the morning of September 12, 2002, the NIO for Strategic and Nuclear Programs had received official guidance from the DCI to begin work on the NIE. The work of assembling and coordinating the NIE was divided primarily between four NIO's: the NIO for Strategic and Nuclear Programs was responsible for the nuclear and ballistic missile portions as well as overall management of the entire NIE, the NIO for Conventional Military Issues was responsible for the chemical warfare (CW) and unmanned aerial vehicle (UAV) portions, and the NIO for Science and Technology was responsible for the biological weapons (BW) portion. The NIO for Near East South Asia (NESA) was also involved in issues regarding regional reactions, interfacing with the NIO for Conventional Military Issues on the doctrine issues, and some terrorism issues, specifically whether Iraq might use terrorists to deliver WMD.

(U) Because of the short time period to prepare the NIE, the NIOs began by drawing language from existing agency and interagency papers. The NIO for Strategic and Nuclear Programs disseminated a draft to the IC agencies for review on September 23, 2002 and held an all-day coordination meeting with IC analysts on September 25, 2002. The NIO for Strategic and Nuclear Programs disseminated a second draft which incorporated the analysts' changes and comments on September 26, 2002. Due to the compressed schedule of this NIE, the NIC did not submit the draft for peer review or to a panel of outside experts. The Vice Chairman of the NIC told Committee staff that because preparation for this NIE involved four NIOs, there was a "virtual peer review," and said that he did not believe that outside experts would have had substantially different views from the NIE, noting that "I think all you could have called in is an amen chorus on this thing, because there was nobody out there with different views." The NIE was approved by a meeting of the full NFIB on October 1, 2002 and printed that day.

(U) The scope note of the NIE said that it "was requested by the Director of Central Intelligence to address the status of and outlook for Iraq's weapons of mass destruction programs" and built on the work and judgments of twelve previous IC products. The NIE contained four sections on specific WMD programs including:

1) Saddam's Pursuit of Nuclear Weapons;
2) Chemical Warfare Program—Rebuilt and Expanding;
3) Biological Warfare Program—Larger Than Before; and
4) Delivery Systems—Iraq Increasing Its Options.

(U) Committee staff examined each of these sections in detail, including the intelligence source reporting underlying the assessments. Committee staff also reviewed previous IC products and assessments from individual IC agencies that discussed Iraq's WMD programs to understand the progression of analysis from the time United Nations inspectors left Iraq in December 1998 until just before the war with Iraq in 2003. The nuclear, biological, chemical and delivery sections of this report discuss the assessments made in those products and the intelligence source reporting the IC analysts used to make their judgments.

3. Overall Conclusions—Weapons of Mass Destruction

(U) Conclusion 1. Most of the major key judgments in the Intelligence Community's October 2002 National Intelligence Estimate (NIE), *Iraq's Continuing Programs for Weapons of Mass Destruction,* either overstated, or were not supported by, the underlying intelligence reporting. A series of failures, particularly in analytic trade craft, led to the mischaracterization of the intelligence.

(U) The major key judgments in the NIE, particularly that Iraq "is reconstituting its nuclear program," "has chemical and biological weapons," was developing an unmanned aerial vehicle (UAV) "probably intended to deliver biological warfare agents," and that "all key aspects—research & development (R&D), production, and weaponization—of Iraq's offensive biological weapons (BW) program are active and that most elements are larger and more advanced than they were before the Gulf War," either overstated, or were not supported by, the underlying intelligence reporting provided to the Committee. The assessments regarding Iraq's continued development of prohibited ballistic missiles were reasonable and did accurately describe the underlying intelligence.

(U) The assessment that Iraq "is reconstituting its nuclear program" was not supported by the intelligence provided to the Committee. The intelligence reporting did show that Iraq was procuring dual-use equipment that had potential nuclear applications, but all of the equipment had conventional military or industrial applications. In addition, none of the intelligence reporting indicated that the equipment was being procured for suspect nuclear facilities. Intelligence reporting also showed that former Iraqi nuclear scientists continued to work at former nuclear facilities and organizations, but the reporting did not show that this cadre of nuclear personnel had recently been regrouped or enhanced as stated in the NIE, nor did it suggest that they were engaged in work related to a nuclear weapons program.

(U) The statement in the key judgments of the NIE that "Baghdad has chemical and biological weapons" overstated both what was known and what intelligence analysts judged about Iraq's chemical and biological weapons holdings. The intelligence reporting did support the conclusion that chemical and biological weapons were within Iraq's technological capability, that Iraq was trying to procure dual-use materials that could have been used to produce these weapons, and that uncertainties existed about whether Iraq had fully destroyed its pre-Gulf War stocks of weapons and precursors. Iraq's efforts to deceive and evade United Nations weapons inspectors and its inability or unwillingness to fully account for pre-Gulf War chemical and biological weapons and precursors could have led analysts to the reasonable conclusion that Iraq may have retained those materials, but intelligence analysts did not have enough information to state with certainty that Iraq "has" these weapons.

([still classified]**)** Similarly, the assessment that "all key aspects—R&D, production, and weaponization—of Iraq's offensive BW program are active and that most elements are larger and more advanced than they were before the Gulf War" was not supported by the underlying intelligence provided to the Committee. Intelligence showed that Iraq was renovating or expanding facilities that had been associated with Iraq's past BW program and was engaged in research that had BW applications, but few reports suggested specifically that the activity was related to BW. Intelligence reports did indicate that Iraq may have had a mobile biological weapons program, but most of the reporting was from a single human intelligence (HUMINT) source to whom the Intelligence Community (IC) never had direct access. It was reasonable for intelligence analysts to be concerned about

the potential weapons applications of Iraq's dual use activities and capabilities. The intelligence reporting did not substantiate an assessment that all aspects of Iraq's BW program "are" larger and more advanced than before the Gulf War, however.

([still classified]**)** The key judgment in the NIE that Iraq was developing a UAV "probably intended to deliver biological warfare agents" also overstated what the intelligence reporting indicated about the mission of Iraq's small UAVs. Numerous intelligence reports confirmed that Iraq was developing a small UAV program [still-classified section missing here], but none of the reports provided to the Committee said that Iraq intended to use the small UAVs to deliver chemical or biological weapons. The Air Force footnote, which stated that biological weapons delivery was a possible mission for the small UAVs, though other missions were more likely, more accurately reflected the body of intelligence reporting.

(U) The failure of the IC to accurately analyze and describe the intelligence in the NIE was the result of a combination of systemic weaknesses, primarily in analytic trade craft, compounded by a lack of information sharing, poor management, and inadequate intelligence collection. Many of these weaknesses, which are described in detail below, have not yet been fully addressed, despite having been identified previously by other inquiry panels, including the *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2002* (2002), *The Intelligence Community's Performance on the Indian Nuclear Tests* (The Jeremiah Report, 1998), and the *Report of the Commission to Assess the Ballistic Missile Threat to the United States* (The Rumsfeld Commission, 1998). The Committee found no evidence that the IC's mischaracterization or exaggeration of the intelligence on Iraq's weapons of mass destruction (WMD) capabilities was the result of political pressure.

(U) Conclusion 2. The Intelligence Community did not accurately or adequately explain to policymakers the uncertainties behind the judgments in the October 2002 National Intelligence Estimate.

(U) One of the key failures in analytic trade craft of the National Intelligence Estimate (NIE) was the failure of the Intelligence Community (IC) to explain the details of the reporting and the uncertainties of both the reliability of some key sources and of intelligence judgments. Intelligence analysts are not only charged with interpreting and assessing the intelligence reporting, but with clearly conveying to policymakers the difference between what intelligence analysts know, what they don't know, what they think, and to make sure that policymakers understand the difference. This articulation of the IC's responsibility to policymakers is widely attributed to Colin Powell when he was serving as the Chairman of the Joint Chiefs of Staff, but the effective communication of judgments has been accepted as a primary analytic function for decades. For example, in 1964, Sherman Kent, considered the founder of intelligence analysis as a profession, wrote about the importance of using appropriate words of estimative probability to "set forth the community's findings in such a way as to make clear to the reader what is certain knowledge and what is reasoned judgment, and within this large realm of judgment what varying degrees of certitude lie behind each key statement."[3]

[3] *Sherman Kent and the Board of National Estimates: Collected Essays,* (Http://www.odci.gov/csi/books/shermankent/inst.html). From 1952 to 1967, Sherman Kent was the Chairman of the Board of National Estimates, which would later become the National Intelligence Council.

(U) At the time the IC drafted and coordinated the NIE on Iraq's weapons of mass destruction (WMD) programs in September 2002, most of what intelligence analysts actually "knew" about Iraq's weapons programs pre-dated the 1991 Gulf War, leaving them with very little direct knowledge about the current state of those programs. Analysts knew that Iraq had active nuclear, chemical, biological, and delivery programs before 1991, and had previously lied to, and was still not forthcoming with, UN weapons inspectors about those programs. The analysts also knew that the United Nations was not satisfied with Iraq's efforts to account for its destruction of all of its pre-Gulf War weapons, precursors, and equipment. Additionally, the analysts knew that Iraq was trying to import dual-use materials and equipment and had rebuilt or was continuing to use facilities that had been associated with Iraq's pre-Gulf War weapons programs, and knew that WMD were likely within Iraq's technological capabilities.

(U) The IC did not know whether Iraq had retained its pre-Gulf War weapons, whether Iraq was intending to use those dual-use materials and facilities for weapons or for legitimate purposes, or even if Iraq's attempts to obtain many of the dual-use goods it had been trying to procure were successful. The IC thought that Iraq had retained its pre-Gulf War weapons and that Iraq was using dual-use materials and facilities to manufacture weapons. While this was a reasonable assessment, considering Iraq's past behavior, statements in the 2002 NIE that Iraq "has chemical and biological weapons," "Iraq has maintained its chemical weapons effort," and "is reconstituting its nuclear weapons program," did not accurately portray the uncertainty of the information. The NIE failed in that it portrayed what intelligence analysts thought and assessed as what they knew and failed to explain the large gaps in the information on which the assessments were based.

([still classified]**)** In the cases in the NIE where the IC did express uncertainty about its assessments concerning Iraq's WMD capabilities, those explanations suggested, in some cases, that Iraq's capabilities were even greater than the NIE judged. For example, the key judgments of the NIE said "we judge that we are seeing only a portion of Iraq's WMD efforts, owing to Baghdad's vigorous denial and deception efforts. Revelations after the Gulf War starkly demonstrate the extensive efforts undertaken by Iraq to deny information." [Still-classified section here.] While this did explain that key information on Iraq's programs was lacking, it suggested that Iraq's weapons programs were probably bigger and more advanced than the IC had judged and did not explain that [classified section here] analysts did not have enough information to determine whether Iraq was hiding activity or whether Iraq's weapons programs may have been dormant.

(U) Accurately and clearly describing the gaps in intelligence knowledge is not only important for policymakers to fully understand the basis for and gaps in analytic assessments, but is essential for policymakers in both the executive and legislative branches to make informed decisions about how and where to allocate Intelligence Community resources to fill those gaps.

(U) Conclusion 3. The Intelligence Community (IC) suffered from a collective presumption that Iraq had an active and growing weapons of mass destruction (WMD) program. This "group think" dynamic led Intelligence Community analysts, collectors and managers to both interpret ambiguous evidence as conclusively indicative of a WMD program as well as ignore or minimize evidence that Iraq did not have active and expanding weapons of mass destruction programs. This presumption was so strong that formalized IC mechanisms established to challenge assumptions and group think were not utilized.

(U) The Intelligence Community (IC) has long struggled with the need for analysts to overcome analytic biases, that is, to resist the tendency to see what they would expect to see in the intelligence reporting. In the case of Iraq's weapons of mass destruction (WMD) capabilities, the Committee found that intelligence analysts, in many cases, based their analysis more on their expectations than on an objective evaluation of the information in the intelligence reporting. Analysts expected to see evidence that Iraq had retained prohibited weapons and that Iraq would resume prohibited WMD activities once United Nations' (UN) inspections ended. This bias that pervaded both the IC's analytic and collection communities represents "group think," a term coined by psychologist Irving Janis in the 1970's to describe a process in which a group can make bad or irrational decisions as each member of the group attempts to conform their opinions to what they believe to be the consensus of the group. IC personnel involved in the Iraq WMD issue demonstrated several aspects of group think: examining few alternatives, selective gathering of information, pressure to conform within the group or withhold criticism, and collective rationalization.

(U) The roots of the IC's bias stretch back to Iraq's pre-1991 efforts to build WMD and its efforts to hide those programs. The fact that Iraq had repeatedly lied about its pre-1991 WMD programs, its continued deceptive behavior, and its failure to fully cooperate with UN inspectors left the IC with a predisposition to believe the Iraqis were continuing to lie about their WMD efforts. This was compounded by the fact that Iraq's pre-1991 progress on its nuclear weapons program had surprised the IC. The role this knowledge played in analysts' thinking is evident in the 2002 National Intelligence Estimate's (NIE) introduction which said, "revelations after the Gulf War starkly demonstrate the extensive efforts undertaken by Iraq to deny information. The revelations also underscore the extent to which limited information fostered underestimates by the Intelligence Community of Saddam's capabilities at that time." This bias was likely further reinforced by the IC's failure to detect the September 11th terrorist plot and the criticism that the Community had not done all it could to "connect the dots."

(U) The IC had long assessed that Iraq maintained its ambitions to obtain WMD, and would seek to resume full WMD efforts once UN sanctions and inspections ended. Accordingly, after UN inspectors left Iraq in 1998, IC analysts began to look for evidence that Iraq was expanding WMD programs. Analysts interpreted ambiguous data as indicative of the active and expanded WMD effort they expected to see. The presumption that Iraq would take advantage of the departure of inspectors to restart its WMD efforts essentially became a hypothesis in search of evidence.

([still classified]**)** The IC's bias was compounded by the fact that prior to 1998, the IC had become heavily dependent on UN information on the state of Iraq's WMD programs. When the IC lost this important information, analysts were forced to rely on less reliable and less detailed sources. For example, [still-classified section here] reporting during UN inspections often described the [still classified]. These reports provided IC analysts with much of the insight [still classified]. Intelligence reporting after inspectors departed relied on less direct sources of information such as satellite imagery of activity at suspect facilities, fragmentary and ambiguous reports of Iraqi dual-use procurement efforts, and reporting of suspicious or prohibited activity from human sources who were no longer in the country. These indirect sources left the IC with few ways to determine the exact nature of suspicious Iraqi activity. The expectation, however, that Iraq would take advantage of the departure of inspectors to resume and expand its WMD programs led analysts to

downplay or ignore the increased uncertainty that came with these less detailed and less reliable sources.

([still classified]**)** The Committee found that the IC had a tendency to accept information which supported the presumption that Iraq had active and expanded WMD programs more readily than information which contradicted it. This was evident in analysts' assessments of Iraq's attempts to procure dual-use materials and activities at dual-use facilities. Dual-use materials and facilities are those which could be used in a WMD program, but which also have conventional military or legitimate civilian applications. The IC properly noted the potential threat embodied in these dual-use capabilities, should they be turned toward WMD purposes, and did an effective job of analyzing [classified section] Iraq's attempts to purchase dual-use equipment and materials to show how they could advance Iraq's WMD capability. But, the IC fell short by accepting most reporting of dual-use material imports or capabilities as intended for WMD programs. Information that contradicted the IC's presumption that Iraq had WMD programs, such as indications in the intelligence reporting that the dual-use materials were intended for conventional or civilian programs, was often ignored. The IC's bias that Iraq had active WMD programs led analysts to presume, in the absence of evidence, that if Iraq could do something to advance its WMD capabilities, it would.

([still classified]**)** Another example of the IC's tendency to reject information that contradicted the presumption that Iraq had active and expanded WMD programs was the return of UN inspectors to Iraq in November 2002. [Classified section.] When these inspections did not find evidence of active Iraqi WMD programs and, in fact, even refuted some aspects of the IC's nuclear and biological assessments, many analysts did not regard this information as significant. For example, the 2002 NIE cited [classified section] Iraq's Amiriyah Serum and Vaccine institute as [still classified] reasons the IC believed the facility was a "fixed dual-use BW agent production" facility. When UN inspectors visited Amiriyah after their return to Iraq in November 2002, however, they did not find any evidence of BW work at the facility [classified section]. Analysts discounted the UN's findings as the result of the inspectors relative inexperience in the face of Iraqi denial and deception. Similarly, when International Atomic Energy Agency (IAEA) inspectors returned to Iraq in late 2002, one of their key lines of work was to investigate Iraq's claims that aluminum tubes it was trying to procure were intended for artillery rockets. The IAEA found that Iraq's claims that the aluminum tubes were intended for artillery rockets was completely consistent with the evidence on the ground in Iraq. The Central Intelligence Agency (CIA) responded to the IAEA's analysis by producing intelligence reports which rejected the IAEA's conclusions. Without giving many details of the IAEA's findings, CIA's analysis suggested that the IAEA was being fooled by Iraq, and reiterated CIA's assessment that the tubes were to be used in uranium centrifuges.

(U) Intelligence analysts' presumption that all dual-use activity was intended for WMD programs recurs throughout the 2002 NIE. Analysts believed that the fact that Iraq often attempted to obtain dual-use materials surreptitiously, through front companies and other illicit means in violation of UN sanctions, indicated that Iraq intended to use those materials for WMD. Analysts argued that Iraq would have no reason to hide itself as the end user of these materials if they were intended for legitimate purposes. However, analysts ignored the fact that Iraq typically used front companies and evaded UN sanctions for imports of purely legitimate goods. Analysts who monitored Iraq's compliance with the Oil for Food Program noted several reasons that Iraq wanted to avoid legitimate channels

for imports including 1) the UN often denied materials needed for legitimate purposes because the materials had WMD applications, 2) using the UN's bureaucratic process was more cumbersome and time consuming than using illicit channels, and 3) transactions using front companies were less transparent, making corruption and profit taking easier for Iraqi managers and officials.

(U) Likewise, analysts were predisposed to identify as suspect any activity by scientists and officials involved in Iraq's pre-1991 WMD programs. While the IC should not have ignored the activity of these people, IC analysts failed to fully consider the possibility that Iraq, having spent significant national resources developing their capabilities, might have been seeking non-WMD purposes to fully employ the idle expertise left over from closed WMD programs.

([still classified]**)** The presumption that Iraq had active WMD programs affected intelligence collectors as well. None of the guidance given to human intelligence collectors suggested that collection be focused on determining *whether* Iraq had WMD. Instead, the requirements assumed that Iraq had WMD, and focused on uncovering those activities and collecting against the extent of Iraq's WMD production and the locations of hidden stocks of weapons. A former manager in the CIA's Iraq WMD Task Force also told Committee staff that, in retrospect, he believes that the CIA tended to discount human intelligence (HUMINT) sources that denied the existence of Iraqi WMD programs as just repeating the Iraqi party line. In fact, numerous interviews with intelligence analysts and documents provided to the Committee indicate that analysts and collectors assumed that sources who denied the existence or continuation of WMD programs and stocks were either lying or not knowledgeable about Iraq's programs, while those sources who reported ongoing WMD activities were seen as having provided valuable information.

([still classified]**)** The presumption that Iraq had active WMD programs was so strong that formalized IC mechanisms established to challenge assumptions and "group think," such as "red teams," "devil's advocacy," and other types of alternative or competitive analysis, were not utilized. The Committee found no evidence that IC analysts, collectors, or managers made any effort to question the fundamental assumptions that Iraq had active and expanded WMD programs, nor did they give serious consideration to other possible explanations for Iraq's failure to satisfy its WMD accounting discrepancies, other than that it was hiding and preserving WMD. The fact that no one in the IC saw a need for such tools is indicative of the strength of the bias that Iraq had active and expanded WMD programs. The Committee does not regard the [still-classified section] analysis on Iraq's aluminum tubes performed by CIA contractors as an attempt to challenge assumptions, but rather as an example of the collective rationalization that is indicative of "group think." The contractors were only provided with information by CIA, did not question agencies about their analysis, were not briefed by other agencies about their analysis, and performed their analysis of a complex intelligence issue in only one day.

(U) The IC's failure to find unambiguous intelligence reporting of Iraqi WMD activities should have encouraged analysts to question their presumption that Iraq had WMD. Instead, analysts rationalized the lack of evidence as the result of "vigorous" Iraqi denial and deception (D&D) efforts to hide the WMD programs that analysts were certain existed. The 2002 NIE's introduction stated that "we judge that we are only seeing a portion of Iraq's WMD efforts owing to Baghdad's vigorous D&D efforts." The intelligence provided to the Committee showed that Iraq was making efforts to hide some activity, but the reporting was not clear about what activity was being hidden or why it was being hidden.

Although the IC lacked unambiguous reporting of either active WMD programs or a vigorous D&D effort to hide WMD programs, the assumptions that Iraq was engaged in both were tied together into a self-reinforcing premise that explained away the lack of strong evidence of either.

(U) Conclusion 4. In a few significant instances, the analysis in the National Intelligence Estimate suffers from a "layering" effect whereby assessments were built based on previous judgments without carrying forward the uncertainties of the underlying judgments.

(U) The Committee defines "layering" as the process of building an intelligence assessment primarily using previous judgments without substantial new intelligence reporting. While this process is a legitimate and often useful analytic tool in making logical connections between intelligence reports and in understanding complex analytic problems, the process can lose its legitimacy when the cumulative uncertainties of the underlying assessments are not factored into or conveyed through the new assessments.

(U) In discussions with the Committee about his experience running the Iraq Survey Group, Dr. David Kay suggested that the IC's mind set before Operation Iraqi Freedom concerning Iraq's weapons of mass destruction (WMD) programs was a train that seemed "to always be going in the same direction." The IC drew on very few pieces of new evidence to reach large conclusions in which new pieces of evidence would accrete to the previous conclusion and pieces that did not fit tended to be thrown aside.

(U) One example of this layering effect occurred in the IC's analysis of Iraq's chemical weapons program. The NIE assessed that Iraq had renewed production of chemical weapons agents and stockpiled as much as 500 metric tons of chemical agent, much of it added in the last year. These assessments were largely based on another assessment, that Iraq may have been engaged in chemical weapons transshipment activity in the spring of 2002. This assessment was largely based on yet another assessment, that the presence of a specific tanker truck was a possible indicator that chemical or biological weapons related activities were occurring. The IC did not make it clear in its latter assessments that its judgments were based on layer upon layer of previous analytic judgments. This gave the reader of the NIE the impression that Iraq's chemical weapons program was advancing and growing, but did not convey that the assessment was based on very little direct or credible intelligence reporting.

([still classified]**)** Similarly, the IC based its judgment that "all key aspects—research & development (R&D), production, and weaponization—of Iraq's offensive biological weapons (BW) program are active and that most elements are larger and more advanced than they were before the Gulf War" primarily on its assessment that Iraq had mobile biological production vans. While this assessment was based on direct intelligence that indicated Iraq had mobile biological production units, the reporting was largely from a single source to whom the Intelligence Community did not have direct access. The Committee believes that the IC's expectation that Iraq would move to mobile biological weapons production, focused their attention on reporting that supported that contention and led them to disregard information that contradicted it. This exemplifies Dr. Kay's concerns that the IC made large new conclusions based on only a few pieces of new evidence that were joined to previous conclusions and that pieces that did not fulfill its expectations tended to be thrown aside.

(U) These are just two, of many, examples of this layering effect the Committee found in the IC's analysis of Iraq's weapons of mass destruction programs. The Committee

recognizes the importance of analysts' ability to perform this type of analytic extrapolation, particularly in trying to "connect the dots" of sometimes seemingly disparate pieces of intelligence. Incorporating and accurately explaining the cumulative underlying uncertainties inherent in that process is equally important, however.

(U) Conclusion 5. In each instance where the Committee found an analytic or collection failure, it resulted in part from a failure of Intelligence Community managers throughout their leadership chains to adequately supervise the work of their analysts and collectors. They did not encourage analysts to challenge their assumptions, fully consider alternative arguments, accurately characterize the intelligence reporting, or counsel analysts who lost their objectivity.

(U) This report describes a variety of serious analytical and collection failures in the Intelligence Community's (IC) work on Iraq's weapons of mass destruction programs. While not in any way diminishing the responsibility of the analysts and collectors that were directly involved, the Committee believes that blame for these failures can not be laid at their feet alone. In each instance, the analysts' and collectors' chains of command in their respective agencies, from immediate supervisors up to the National Intelligence Council and the Director of Central Intelligence, all share responsibility for not encouraging analysts to challenge their assumptions, fully consider alternative arguments or accurately characterize the intelligence reporting. They failed to adequately question and challenge analysts about their assessments, and, most importantly, to recognize when analysts had lost their objectivity and take corrective action. It seems likely that these failures of management and leadership resulted at least in part as a result of the fact that the Intelligence Community's chain of command shared with its analysts and collectors the same "group think" presumption that Iraq had active and expanded weapons of mass destruction programs.

(U) Conclusion 6. The Committee found significant short-comings in almost every aspect of the Intelligence Community's human intelligence collection efforts against Iraq's weapons of mass destruction activities, in particular that the Community had no sources collecting against weapons of mass destruction in Iraq after 1998. Most, if not all, of these problems stem from a broken corporate culture and poor management, and will not be solved by additional funding and personnel.

(U) The Committee's review into the prewar intelligence concerning Iraq's weapons of mass destruction programs has entailed an unprecedented outside examination of a broad range of the Intelligence Community's (IC) human intelligence (HUMINT) operations. The Committee found significant short-comings in almost every aspect of these operations.

([still classified]**)** From 1991 to 1998, the IC relied too heavily on United Nations (UN) inspectors to collect information about Iraq's weapons of mass destruction programs and did not develop a sufficient unilateral HUMINT collection effort targeting Iraq to supplement UN-collected information and to take its place upon the departure of the UN inspectors. While the UN inspection process provided a valuable source of information, the IC should have used the time when inspectors were in Iraq to plan for the possibility that inspectors would leave and to develop sources who could continue to report after inspectors left.

([still classified]**)** Because the United States lacked an official presence inside Iraq, the Intelligence Community depended too heavily on defectors and foreign government services to obtain HUMINT information on Iraq's weapons of mass destruction activities.

While these sources had the potential to provide some valuable information, they had a limited ability to provide the kind of detailed intelligence about current Iraqi weapons of mass destruction efforts sought by U.S. policymakers. Moreover, because the Intelligence Community did not have direct access to many of these sources, their credibility was difficult to assess and was often left to the foreign government services to judge. Intelligence Community HUMINT efforts against a closed society like Iraq prior to Operation Iraqi Freedom were hobbled by the Intelligence Community's dependence on having an official U.S. presence in-country to mount clandestine HUMINT collection efforts.

(U) When UN inspectors departed Iraq, the placement of HUMINT agents and the development of unilateral sources inside Iraq were not top priorities for the Intelligence Community. The Intelligence Community did not have a single HUMINT source collecting against Iraq's weapons of mass destruction programs in Iraq after 1998. The Intelligence Community appears to have decided that the difficulty and risks inherent in developing sources or inserting operations officers into Iraq outweighed the potential benefits. The Committee found no evidence that a lack of resources significantly prevented the Intelligence Community from developing sources or inserting operations officers into Iraq.

([still classified]) [Still-classified section.] When Committee staff asked why the CIA had not considered placing a CIA officer in Iraq years before Operation Iraqi Freedom to investigate Iraq's weapons of mass destruction programs, a CIA officer said, "because it's very hard to sustain . . . it takes a rare officer who can go in . . . and survive scrutiny [still classified] for along time." The Committee agrees that such operations are difficult and dangerous, but they should be within the norm of the CIA's activities and capabilities. Senior CIA officials have repeatedly told the Committee that a significant increase in funding and personnel will be required to enable to the CIA to penetrate difficult HUMINT targets similar to prewar Iraq. The Committee believes, however, that if an officer willing and able to take such an assignment really is "rare" at the CIA, the problem is less a question of resources than a need for dramatic changes in a risk averse corporate culture.

(U) Problems with the Intelligence Community's HUMINT efforts were also evident in the Intelligence Community's handling of Iraq's alleged efforts to acquire uranium from Niger. The Committee does not fault the CIA for exploiting the access enjoyed by the spouse of a CIA employee traveling to Niger. The Committee believes, however, that it is unfortunate, considering the significant resources available to the CIA, that this was the only option available. Given the nature of rapidly evolving global threats such as terrorism and the proliferation of weapons and weapons technology, the Intelligence Community must develop means to quickly respond to fleeting collection opportunities outside the Community's established operating areas. The Committee also found other problems with the Intelligence Community's follow-up on the Iraq-Niger uranium issue, including a half-hearted investigation of the reported storage of uranium in a warehouse in Benin, and a failure, to this day, to call a telephone number, provided by the Navy, of an individual who claimed to have information about Iraq's alleged efforts to acquire uranium from Niger.

([still classified]) The Committee also found that the Defense HUMINT Service (DHS) demonstrated serious lapses in its handling of the HUMINT source code named CURVE BALL, who was the principle source behind the Intelligence Community's assessments that Iraq had a mobile biological weapons program. The DHS had primary responsibility for handling the Intelligence Community's interaction with the [still-classified section] debriefers that were handling CURVE BALL, but the DHS officers that

were involved in CURVE BALL's case limited themselves to a largely administrative role, translating and passing along reports [lengthy still-classified section here] analysts do not have the benefit of the regular interaction with sources or, in this case, CURVE BALL's debriefers, that could have allowed them to make judgments about the reliability of source reporting.

(U) Another significant problem found by the Committee is the fact that the CIA continues to excessively compartment sensitive HUMINT reporting and fails to share important information about HUMINT reporting and sources with Intelligence Community analysts who have a need to know. In the years before Operation Iraqi Freedom, the CIA protected its Iraq weapons of mass destruction sources so well that some of the information they provided was kept from the majority of analysts with a legitimate need to know. The biological weapons and delivery sections of this report discuss at length the CIA's failure to share important information about source reporting on Iraq's alleged mobile biological weapons program and unmanned aerial vehicle (UAV) program that left analysts and policymakers with an incomplete and, at times, misleading picture of these issues.

(U) The process by which the Intelligence Community calculates the benefits and risks of sharing sensitive human intelligence is skewed too heavily toward withholding information. This issue has been raised repeatedly with the Intelligence Community, particularly after the lack of information sharing was found to have played a key role in the intelligence failures of 9/11. The Committee believes that the Intelligence Community must reconsider whether the risks of expanding access to *cleared* analysts are truly greater than the risks of keeping information so tightly compartmented that the analysts who need it to make informed judgments are kept in the dark.

(U) Conclusion 7. The Central Intelligence Agency (CIA), in several significant instances, abused its unique position in the Intelligence Community, particularly in terms of information sharing, to the detriment of the Intelligence Community's prewar analysis concerning Iraq's weapons of mass destruction programs.

(U) The Intelligence Community is not a level playing field when it comes to the competition of ideas in intelligence analysis. The Director of Central Intelligence's (DC's) responsibility, established by the National Security Act of 1947, to coordinate the nation's intelligence activities and correlate, evaluate, and disseminate intelligence that affects national security, provides the CIA with a unique position in the Intelligence Community. The fact that the DCI is the head of the CIA and head of the Intelligence Community, the principal intelligence advisor to the President, and is responsible for protecting intelligence sources and methods, provides the CIA with unique access to policymakers and unique control of intelligence reporting. This arrangement was intended to coordinate the disparate elements of the Intelligence Community in order to provide the most accurate and objective analysis to policymakers. The Committee found that in practice, however, in the case of the Intelligence Community's analysis of Iraq's weapons of mass destruction programs, this arrangement actually undermined the provision of accurate and objective analysis by hampering intelligence sharing and allowing CIA analysts to control the presentation of information to policymakers, and exclude analysis from other agencies.

(U) The Committee found in a number of cases that significant reportable intelligence was sequestered in CIA Directorate of Operations (DO) cables, distribution of sensitive intelligence reports was excessively restricted, and CIA analysts were often provided with "sensitive" information that was not made available to analysts who worked the same issues at other all-source analysis agencies. These restrictions, in several cases, kept

information from analysts that was essential to their ability to make fully informed judgments. Analysts cannot be expected to formulate and present their best analysis to policymakers while having only partial knowledge of an issue.

([still-classified]**)** For example, important information concerning the reliability of two of the main sources on Iraq's alleged mobile biological weapons program was not available to most Iraq biological weapons analysts outside the CIA. Some analysts at other agencies were aware of some of the credibility concerns about the sources, but the CIA's DO did not disseminate cables throughout the Intelligence Community that would have provided this information to all Iraq biological weapons analysts. [Still-classified section here.]

([still classified]**)** The CIA also failed to share important information about Iraq's UAV software procurement efforts with other intelligence analysts. The CIA did share sensitive information that indicated Iraq [still-classified section here] was trying to obtain mapping software that could only be used for mapping in the U.S. This suggested to many analysts that Iraq may have been intending to use the software to target the U.S. The CIA failed to pass on additional information, until well after the coordination and publication of the National Intelligence Estimate (NIE). [Still-classified section here.] This information was essential for analysts to make fully informed judgments about Iraq's intentions to target the U.S.

(U) In some cases CIA analysts were not open to fully considering information and opinions from other intelligence analysts or creating a level playing field in which outside analysts fully participated in meetings or analytic efforts. This problem was particularly evident in the case of the CIA's analysis of Iraq's procurement of aluminum tubes during which the Committee believes the agency lost objectivity and in several cases took action that improperly excluded useful expertise from the intelligence debate. For example, the CIA performed testing of the tubes without inviting experts from the Department of Energy (DOE) to participate. A CIA analyst told Committee staff that the DOE was not invited "because we funded it. It was our testing. We were trying to prove some things that we wanted to prove with the testing. It wasn't a joint effort." The Committee believes that such an effort should never have been intended to prove what the CIA wanted to prove, but should have been a Community effort to get to the truth about Iraq's intended use for the tubes. By excluding DOE analysts, the Intelligence Community's nuclear experts, the CIA was not able to take advantage of their potentially valuable analytic insights. In another instance, an independent Department of Defense (DOD) rocket expert told the Committee that he did not think the CIA analysts came to him for an objective opinion, but were trying "to encourage us to come up with [the] answer" that the tubes were not intended to be used for a rocket program.

(U) The Committee also found that while the DCI was supposed to function as both the head of the CIA and the head of the Intelligence Community, in many instances he only acted as head of the CIA. For example, the DCI told the Committee that he was not aware that there were dissenting opinions within the Intelligence Community on whether Iraq intended use the aluminum tubes for a nuclear program until the NIE was drafted in September 2002, despite the fact that intelligence agencies had been fervently debating the issue since the spring of 2001. While the DCI, as the President's principal intelligence advisor, should provide policymakers, in particular the President, with the best analysis available from throughout the Intelligence Community, the DCI told Committee staff that he does not even expect to learn of dissenting opinions "until the issue gets joined" through interagency coordination of an NIE. This means that contentious debate about

significant national security issues can go on at the analytic level for months, or years, without the DCI or senior policymakers being informed of any opinions other than those of CIA analysts. In addition, the Presidential Daily Briefs (PDBs) are prepared by CIA analysts and are presented by CIA briefers who may or may not include an explanation of alternative views from other intelligence agencies. Other Intelligence Community agencies essentially must rely on the analysts who disagree with their positions to accurately convey their analysis to the nation's most senior policymakers.

(U) These factors worked together to allow CIA analysts and officials to provide the agency's intelligence analysis to senior policymakers without having to explain dissenting views or defend their analysis from potential challenges from other Intelligence Community agencies. The Committee believes that policymakers at all levels of government and in both the executive and legislative branches would benefit from understanding the full range of analytic opinions directly from the agencies who hold those views, or from truly impartial representatives of the entire Intelligence Community.

C. IRAQ'S TIES TO TERRORISM

(U) The terrorism related sections of the report recount the Committee's efforts to evaluate the quantity and quality of the intelligence underlying prewar assessments. Each section contains it own set of conclusions. There is also a separate section on the issue of objectivity and whether analysts were pressured to reach specific conclusions to support a particular policy objective. Unlike the WMD sections of the report, in some instances, the issue of accuracy has been addressed as post-war reporting has become available.

(U) Because there was no National Intelligence Estimate specifically focused on Iraq's ties to terrorism, the Committee focused its work primarily the January 2003 Intelligence Report entitled *Iraqi Support for Terrorism.* This intelligence assessment was drafted by the Director of Central Intelligence's (DCI) Counterterrorist Center (CTC). (The CTC includes analysts from across the Intelligence Community.) *Iraqi Support for Terrorism* was first published for a limited executive audience in September 2002 under the same title. There were a few changes made to the January 2003 version of the document including the addition of new information that had been collected following the September publication. The Committee chose to evaluate it as the IC's most comprehensive product on the subject because the January 2003 paper was the most current version and was disseminated to a much wider audience.

(U) To complete this section of the report, the Committee's staff interviewed a total of sixty-two individuals and reviewed more than 1,000 documents provided by the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the State Department's Bureau of Intelligence and Research (INR), and the Federal Bureau of Investigation (FBI). To gain an in-depth understanding of the Intelligence Community (IC) and CTC collection posture, Committee staff received a briefing from the Assistant Director of Central Intelligence for Collection (ADCI/C) and met with two former heads of the DCI's Counterterrorist Center (CTC). Committee staff interviewed analysts from the CTC, DIA, and FBI who were responsible for assessing Iraq's links to al-Qaida. Committee staff also met with National Security Agency (NSA) employees who collected and analyzed signals intelligence (SIGINT) related to Iraq's links to terrorism. To address analytical objectivity and allegations concerning the politicization of the intelligence process, Committee staff received a briefing from the CIA Ombudsman for Politicization and interviewed IC analysts

who interacted with, *inter alia,* personnel from the Office of the Under Secretary of Defense for Policy (OUSDP).

(U) In addition to reviewing activities specifically relating to Iraq's links to terrorism, the Committee staff participated in a briefing to the Committee by the Under Secretary of Defense for Policy and in a Committee hearing with the former Special Advisor to the DCI on Iraq's Weapons of Mass Destruction. On each occasion, the Committee raised the issue of Iraq's links to terrorism.

(U) Intelligence from the 1960s and 1970s first established the link between Iraq and terrorism, resulting in Iraq's inclusion in the State Department's 1979 list of State Sponsors of Terrorism. The State Department removed Iraq from the list in 1982.[4] Iraq returned to the list in 1990 based upon intelligence information linking the regime to acts of terrorism conducted by the Iraqi Intelligence Service (IIS) and its support for Palestinian terrorists. The first intelligence reports suggesting links between Iraq and al-Qaida emerged in the mid-1990s. The IC continues to receive reporting on these links from detainees and document exploitation.

(U) While the nature of the intelligence reporting produced or obtained by the IC has not changed dramatically in the past decade, there has been a significant shift in the way IC analysts evaluate reporting regarding terrorism, particularly in the aftermath of the September 11 attacks. CIA officials interviewed by Committee staff indicated that, following the terrorist attacks of September 11, 2001, the trade craft of terrorism analysis shifted and analysts now feel obligated to make more conclusive assessments regardless of the quality of the available intelligence. In this new analytic environment analysts cannot set aside intelligence reports because the information does not fit within the context of their prior knowledge or because the report has not been corroborated. The CIA Deputy Director for Intelligence (DDI), describing the unique nature of terrorism analysis, said, "... terrorism analysis is just fundamentally different on some issues." She commented further that:

> Sometimes it is the walk-in who has the best information about the impending attack. What we teach people in trade craft is that you want to get a report. It's preferable that that report come from a fully-vetted source whose information is from a long-established reporting record, has direct access and you've been able to corroborate it somehow. That's what you would ideally like and that's what you ideally teach analysts to look for. But with terrorism you can't dismiss the walk-in.

The Deputy Director of the CTC's Office of Terrorism Analysis noted that this is the most difficult issue he has encountered in his eighteen years of intelligence analysis. He also stated that:

> On the other hand, I would also say that we've encouraged and developed a sense of trade craft specifically on terrorism that says push the envelope because the implications are so high and because we have to acknowledge up front that, unlike in some other cases, some other lines of analysis, that we have to accept that often our information is going to be fragmentary and, if we wait too long to reach conclusions, we might make a mistake.

[4] The 1982 State Department publication *Patterns of Global Terrorism* explained Iraq's removal from the list of State Sponsors of Terrorism in the following manner: "The Iraqi Government has reduced support to non-Palestinian groups, thereby moving closer to the policies of its moderate Arab neighbors."

(U) The focus of the Committee's terrorism review, *Iraqi Support for Terrorism,* addressed four main issues:

- terrorist activities conducted by the IIS;
- Iraqi support for terrorist activities conducted by regional terrorist groups;
- Iraqi contacts with al-Qaida; and,
- potential Iraqi use of terrorism in the event of a war with the United States.

(U) Committee staff evaluated each of these and other issues including the intelligence source reporting underlying the assessments. The terrorism related sections of this report discuss the assessments and the intelligence reporting in detail.

1. Overall Conclusions—Terrorism

(U) Conclusion 8. Intelligence Community analysts lack a consistent post-September 11 approach to analyzing and reporting on terrorist threats.

(U) Though analysts have been wrong on major issues in the past, no previous intelligence failure has been so costly as the September 11 attacks. As the Deputy Director of Intelligence (DDT) explained during an interview with Committee staff, terrorist threat analysts now use a different type of trade craft than generally employed by political, leadership or regional analysts. Threat analysts are encouraged to "push the envelope" and look at various possible threat scenarios that can be drawn from limited and often fragmentary information. As a result, analysts can no longer dismiss a threat as incredible because they cannot corroborate it. They cannot dismiss what may appear to be the rantings of a walk-in until additional vetting shows those stories to be fabricated.

(U) To compensate for the fragmentary nature of the reporting on Iraq's potential links to al-Qaida, Intelligence Community (IC) analysts included as much detail as they could about the nature of the sources and went to great lengths to describe their analytic approach to the problem. For example, where information was limited to a single or untested source or to a foreign government service, a source description was provided. As discussed in more detail in the body of this report, a "Scope Note" was incorporated in each product to describe the analytic approach the drafters had taken to address the issue. In *Iraq and al-Qaida: Interpreting a Murky Relationship,* the Scope Note explained that the authors had purposefully taken an aggressive approach to interpreting the available data. In both the September 2002 and January 2003 versions of *Iraqi Support for Terrorism,* the Scope Note did not describe an analytic approach, but rather it highlighted the gaps in information and described the analysts' understanding of the Iraq–al-Qaida relationship as "evolving."

(U) Though the Committee understands the need for different analytical approaches and expressions of competing viewpoints, the IC should have considered that their readership would not necessarily understand the nuance between the first "purposely aggressive" approach and a return, in *Iraqi Support for Terrorism,* to a more traditional analysis of the reporting concerning Iraq's links to al-Qaida. A consistent approach in both assessments which carefully explained the intelligence reports and then provided a spectrum of possible conclusions would have been more useful and would have assisted policymakers in their public characterizations of the intelligence.

(U) Conclusion 9. Source protection policies within the Intelligence Community direct or encourage reports officers to exclude relevant detail about the nature of

their sources. As a result, analysts community-wide are unable to make fully informed judgments about the information they receive, relying instead on nonspecific source lines to reach their assessments. Moreover, relevant operational data is nearly always withheld from analysts, putting them at a further analytical disadvantage.

(U) A significant portion of the intelligence reporting that was used to evaluate whether Iraq's interactions with al-Qaida operatives constituted a relationship was stripped of details prior to being made available to analysts community-wide. Source information and operational detail was provided only to Central Intelligence Agency (CIA) analysts. This lack of information sharing limited the level of discussion and debate that should have taken place across the Community on this critical issue. While in the case of Iraq's links to terrorism, the final analysis has proven, thus far, to have been accurate and not affected by a lack of relevant source or operational detail, we cannot rely on this system in the future. Until changes are made concerning how and when source information is made available to analysts, we run the risk of missing critical data that might provide early warning.

(U) The absence of source and operational detail affects not only analysts, but policymakers as well. The Committee found that policymakers took an active role by personally examining individual intelligence reports for themselves. If this trend continues, it is even more important that such relevant detail be provided.

([still-classified]) **Conclusion 10. The Intelligence Community relies too heavily on foreign government services and third party reporting, thereby increasing the potential for manipulation of U.S. policy by foreign interests.**

([still-classified]) Due to the lack of unilateral sources on Iraq's links to terrorist groups like al-Qaida [still-classified section here], the Intelligence Community (IC) relied too heavily on foreign government service reporting and sources to whom it did not have direct access to determine the relationship between Iraq and [still-classified] terrorist groups. While much of this reporting was credible, the IC left itself open to possible manipulation by foreign governments and other parties interested in influencing U.S. policy. The Intelligence Community's collectors must develop and recruit unilateral sources with direct access to terrorist groups to confirm, complement or confront foreign government service reporting on these critical targets.

(U) Conclusion 11. Several of the allegations of pressure on Intelligence Community (IC) analysts involved repeated questioning. The Committee believes that IC analysts should expect difficult and repeated questions regarding threat information. Just as the post 9/11 environment lowered the Intelligence Community's reporting threshold, it has also affected the intensity with which policymakers will review and question threat information.

(U) A number of the individuals interviewed by the Committee in conducting its review stated that Administration officials questioned analysts repeatedly on the potential for cooperation between Saddam Hussein's regime and al-Qaida. Though these allegations appeared repeatedly in the press and in other public reporting on the lead-up to the war, no analyst questioned by the Committee stated that the questions were unreasonable, or that they were encouraged by the questioning to alter their conclusions regarding Iraq's links to al-Qaida.

(U) In some cases, those interviewed stated that the questions had forced them to go back and review the intelligence reporting, and that during this exercise they came across information they had overlooked in initial readings. The Committee found that this process—the policymakers probing questions—actually improved the Central Intelligence

Agency's (CIA) products. The review revealed that the CIA analysts who prepared *Iraqi Support for Terrorism* made careful, measured assessments which did not overstate or mischaracterize the intelligence reporting upon which it was based.

(U) The Committee also found that CIA analysts are trained to expect questions from policymakers, and to tailor their analysis into a product that is useful to them. In an Occasional Paper on improving CIA analytic performance, written by a Research Fellow at the Sherman Kent Center, the fellow states:

> If the mission of intelligence analysis is to inform policymaking—to help the U.S. government anticipate threats and seize opportunities—then customization of analysis is the essence of the professional practice, not a defilement of it (i.e., politicization). **In effect there is no such thing as an unprofessional policymaker question for intelligence to address so long as the answer reflects professional analytic trade craft (e.g., tough-minded weighing of evidence and open-minded consideration of alternatives).** (Emphasis added)

(U) The same Research Fellow commented on strategic warning stating, "Key to the warning challenge is that the substantive uncertainty surrounding threats to U.S. interests requires analysts, and policymakers, to make judgments that are inherently vulnerable to error." This vulnerability has never been so apparent as in the failure to detect and deter the attacks on September 11, 2001. While analysts cannot dismiss a threat because at first glance it seems unreasonable or it cannot be corroborated by other credible reporting, policymakers have the ultimate responsibility for making decisions based on this same fragmentary, inconclusive reporting. If policymakers did not respond to analysts' caveated judgments with pointed, probing questions, and did not require them to produce the most complete assessments possible, they would not be doing their jobs.

GLOSSARY

ACCM	Alternative or Compensatory Control Measure
AFIO	Association of Former Intelligence Officers
AG	Attorney General
Aman	Agaf ha-Modi'in (Israeli military intelligence)
ANC	African National Congress
BDA	Battle Damage Assessment
BfV	Bundesamt für Verfassungsschutz (German equivalent of the FBI)
BMD	Ballistic Missile Defense
BND	Bundesnachrichtendienst (German foreign intelligence service)
BSO	Black September Organization
BW	Biological Weapons
CA	Covert Action
CAS	Covert Action Staff (CIA)
CBW	Chemical/Biological Warfare
CCP	Consolidated Cryptographic Program
CDA	Congressionally Directed Action
CE	Counterespionage
CHAOS	Code name for CIA illegal domestic spying
CI	Counterintelligence
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CIG	Central Intelligence Group
CMS	Community Management Staff
CNC	Crime and Narcotics Center (CIA)

COINTELPRO	FBI Counterintelligence Program
COMINT	Communications Intelligence
Corona	Codename for first U.S. spy satellite system
COS	Chief of Station (CIA)
COSPO	Community Open Source Program Office
CPA	Covert Political Action
CPSU	Communist Party of the Soviet Union
CSI	Committee on Intelligence Services (Britain)
CT	Counterterrorism
CTC	Counterterrorism Center (CIA)
CW	Chemical Weapons
D & D	Denial and Deception
DARP	Defense Airborne Reconnaissance Program
DAS	Deputy Assistant Secretary
DBA	Dominant Battlefield Awareness
DC	Deputies Committee (NSC)
DCD	Domestic Contact Division (CIA)
DCI	Director of Central Intelligence
D/CIA	Director of Central Intelligence Agency
DDA	Deputy Director of Administration (CIA)
DDCI	Deputy Director for Central Intelligence (DDCI)
DD/CIA	Deputy Director, Central Intelligence Agency
DDO	Deputy Director for Operations (CIA)
DDP	Deputy Director for Plans (CIA)
DDS&T	Deputy Director for Science and Technology (CIA)
DEA	Drug Enforcement Administration
DGSE	Directorie Génerale de la Sécurité Extérieure (French intelligence service)
DHS	Department of Homeland Security
DI	Directorate of Intelligence (CIA)
DIA	Defense Intelligence Agency
DIA/Humint	Defense Humint Service
DINSUM	*Defense Intelligence Summary*
DNI	Director of National Intelligence
DO	Directorate of Operations
DoD	Department of Defense
DOD	Domestic Operations Division (CIA)
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Treasury
DOS	Department of State
DP	Directorate of Plans (CIA)
DST	Directoire de Surveillance Territore (France)
ECHR	European Convention of Human Rights

ELINT	Electronic Intelligence
ENIGMA	Code machine used by the Germans during World War II
EO	Executive Order
EOP	Executive Office of the President
ETF	Environmental Task Force (CIA)
FARC	Fuerzas Armadas Revolucionarias in Colombia
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FISA	Foreign Intelligence Surveillance Act (1978)
FNLA	National Front for the Liberation of Angola
FOIA	Freedom of Information Act
FRD	Foreign Resources Division (CIA)
FSB	Federal'naya Sluzba Besnopasnoti (Federal Security Service, Russia)
GAO	General Accountability Office (Congress)
GCHQ	Government Communications Headquarters (the British NSA)
GEO	Geosynchronous Orbit
GEOINT	Geospatial Intelligence
GRU	Soviet Military Intelligence
GSG	German Counterterrorism Service
HEO	High Elliptical Orbit
HPSCI	House Permanent Select Committee on Intelligence
HUAC	House Un-American Activities Committee
HUMINT	Human Intelligence (assets)
I & W	Indicators and Warning
IAEA	International Atomic Energy Agency
IAF	Israel Air Force
IC	Intelligence Community
ICS	Intelligence Community Staff
IDF	Israeli Defense Force
IG	Inspector General
IMINT	Imagery Intelligence (photographs)
INR	Bureau of Intelligence and Research (Department of State)
INTELINK	An intelligence community computer information system
INTs	Collection disciplines (IMINT, SIGINT, OSINT, HUMINT, MASINT)
IOB	Intelligence Oversight Board (White House)
ISA	Israeli Security Agency
ISC	Intelligence and Security Committee (U.K.)
ISI	Inter-Services Intelligence (Pakistani intelligence agency)
IT	Information Technology
JCAE	Joint Committee on Atomic Energy
JCS	Joint Chiefs of Staff
JIC	Joint Intelligence Committee (U.K.)

JSOC	Joint Special Operations Command
JSTARS	Joint Surveillance Target Attack Radar Systems
KGB	Soviet Secret Police
KH	Keyhole (satellite)
LTTE	Tamil Tigers of Tamil Elam
MAGIC	Allied code-breaking operations against the Japanese in the World War II
MASINT	Measurement and Signatures Intelligence
MI5	Security Service (U.K.)
MI6	Secret Intelligence Service (U.K.)
MON	Memoranda of Notification
MONGOOSE	Code name for CIA covert actions against Fidel Castro of Cuba (1961–62)
Mossad	Israeli Intelligence Service
MPLA	Popular Movement for the Liberation of Angola
NAACP	National Association for the Advancement of Colored People
NBC	Nuclear, Biological, and Chemical (Weapons)
NCS	National Clandestine Service
NCIC	National Counterintelligence Center
NCTC	National Counterterrorism Center
NED	National Endowment for Democracy
NFIB	National Foreign Intelligence Board
NFIC	National Foreign Intelligence Council
NFIP	National Foreign Intelligence Program
NGA	National Geospatial-Intelligence Agency
NGO	Nongovernmental organization
NIA	National Intelligence Authority
NIC	National Intelligence Council
NID	*National Intelligence Daily*
NIE	National Intelligence Estimate
NIO	National Intelligence Officer
NOC	Nonofficial Cover
NPIC	National Photographic Interpretation Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council (White House)
NSCID	National Security Council Intelligence Directive
NTM	National Technical Means
OB	Order of Battle
OC	Official Cover
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
ONI	Office of Naval Intelligence

OPC	Office of Policy Coordination
OSD	Office of the Secretary of Defense
OSINT	Open-Source Intelligence
OSS	Office of Strategic Services
P & E	Processing and Exploitation
PDB	*President's Daily Brief*
PFIAB	President's Foreign Intelligence Advisory Board (White House)
PFLP	Popular Front for the Liberation of Palestine
PIJ	Palestinian Islamic Jihad
PLO	Palestine Liberation Organization
PM	Paramilitary
PRO	Public Record Office (U.K.)
RADINT	Radar Intelligence
RFE	Radio Free Europe
RL	Radio Liberty
SA	Special Activities Division (DO/CIA)
SAS	Special Air Service (U.K.)
SBS	Special Boat Service (U.K.)
SDO	Support to Diplomatic Operations
SHAMROCK	Code name for illegal NSA interception of cables
SIG	Senior Interagency Group
SIGINT	Signals Intelligence
SIS	Secret Intelligence Service (U.K., also known as MI6)
SISDE	Italian Intelligence Service
SMO	Support to Military Operations
SMS	Secretary's *Morning Summary* (Department of State)
SNIE	Special National Intelligence Estimate
SO	Special Operations (CIA)
SOCOM	Special Operations Command (Department of Defense)
SOE	Special Operations Executive (U.K.)
SOG	Special Operations Group (DO/CIA)
SOVA	Office of Soviet Analysis (CIA)
SSCI	Senate Select Committee on Intelligence
SVR	Russian Foreign Intelligence Service
TECHINT	Technical Intelligence
TELINT	Telemetery Intelligence
TIARA	Tactical Intelligence and Related Activities
TPED	Tasking, Processing, Exploitation, and Dissemination
UAV	Unmanned Aerial Vehicle (drone)
ULTRA	Code name for the Allied operation that deciphered the German ENIGMA code in World War II
UN	United Nations
UNITA	National Union for the Total Independence of Angola

UNSCOM	United Nations Special Commission
USIB	United States Intelligence Board
USTR	United States Trade Representative
VCI	Viet Cong Infrastructure
VENONA	Code name for SIGINT intercepts against Soviet spying in America
VOA	Voice of America
VX	A deadly nerve agent used in chemical weapons
WMD	Weapons of mass destruction

INDEX

ABOUT THE EDITOR AND CONTRIBUTORS

EDITOR

Loch K. Johnson is Regents Professor of Public and International Affairs at the University of Georgia and author of several books and over 100 articles on U.S. intelligence and national security. His books include *The Making of International Agreements* (1984); *A Season of Inquiry* (1985); *Through the Straits of Armageddon* (1987, coedited with Paul Diehl); *Decisions of the Highest Order* (1988, coedited with Karl F. Inderfurth); *America's Secret Power* (1989); *Runoff Elections in the United States* (1993, coauthored with Charles S. Bullock III); *America as a World Power* (1995); *Secret Agencies* (1996); *Bombs, Bugs, Drugs, and Thugs* (2000); *Fateful Decisions* (2004, coedited with Karl F. Inderfurth); *Strategic Intelligence* (2004, coedited with James J. Wirtz); *Who's Watching the Spies?* (2005, coauthored with Hans Born and Ian Leigh); *American Foreign Policy* (2005, coauthored with Daniel Papp and John Endicott); and *Seven Sins of American Foreign* Policy (2007). He has served as special assistant to the chair of the Senate Select Committee on Intelligence (1975–76), staff director of the House Subcommittee on Intelligence Oversight (1977–79), and special assistant to the chair of the Aspin-Brown Commission on Intelligence (1995–96). In 1969–70, he was an American Political Science Association Congressional Fellow. He has served as secretary of the American Political Science Association and President of the International Studies Association, South. Born in New Zealand and educated at the University of California, Johnson has taught at the University of Georgia since 1979, winning its Meigs Professorship for meritorious teaching and its Owens Award for outstanding accomplishments in the field of social science research. In 2000, he led the founding of the School of Public and

International Affairs at the University of Georgia. He is the senior editor of the international journal *Intelligence and National Security*.

CONTRIBUTORS

Matthew M. Aid is Managing Director in the Washington, DC, office of Citigate Global Intelligence and Security and coeditor of *Secrets of Signals Intelligence During the Cold War and Beyond* (2001).

James E. Baker sits on the U.S. Court of Appeals for the Armed Forces. He previously served as Special Assistant to the President and Legal Adviser to the National Security Council and as Deputy Legal Adviser to the NSC. He has also served as Counsel to the President's Foreign Intelligence Advisory Board, an attorney at the Department of State, a legislative aide to Senator Daniel Patrick Moynihan, and as a Marine Corps infantry officer. He is the coauthor with Michael Reisman of *Regulating Covert Action* (Yale University Press, 1992).

David M. Barrett is Associate Professor of Political Science at Villanova University and author of *Congress and the CIA* (Kansas, 2005).

Hans Born is a senior fellow in democratic governance of the security sector at the Geneva Centre for Democratic Control of the Armed Forces (DCAF). He is an external member of the crisis management and security policy faculty of the Federal Institute of Technology and a guest lecturer on governing nuclear weapons at the UN Disarmament Fellowship Programme. He has written, co-authored, and co-edited various books on international relations and security policy, including the Inter-Parliamentary Union Handbook on *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices* (Geneva: IPU/DCAF, 2003, translated in 30 languages); *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005, translated in 10 languages); *Who is Watching the Spies? Establishing Intelligence Agency Accountability* (Dulles, VA: Potomac Publishers, 2005); *Civil-Military Relations in Europe: Learning from Crisis and Institutional Change* (London: Routledge, 2006); and *The Double Democratic Deficit: Parliamentary Accountability and the Use of Force under International Auspices* (London: Ashgate Publishers: Aldershot).

A. Denis Clift is President of the Department of Defense Joint Military Intelligence College. He was born in New York City and educated at Friends Seminary, Phillips Exeter Academy (1954), Stanford University (B.A., 1958), and the London School of Economics and Political Science (M.Sc., 1967). He began a career of public service as a naval officer in the Eisenhower and Kennedy administrations and has served in military and civilian capacities in ten administrations, including thirteen successive years in the Executive Office of the President and the White House. From 1971–76, he served on the National Security

Council staff. From 1974–76, he was head of President Ford's National Security Council staff for the Soviet Union and Eastern and Western Europe. From 1977–81, he was Assistant for National Security Affairs to the Vice President. From 1991–94, he was Chief of Staff, Defense Intelligence Agency. From 1963–66, he was the editor of the U.S. Naval Institute *Proceedings*. His published fiction and nonfiction include the novel *A Death in Geneva* (Ballantine Books, Random House), *Our World in Antarctica* (Rand McNally), *With Presidents to the Summit* (George Mason University Press), and *Clift Notes: Intelligence and the Nation's Security* (JMIC Writing Center Press).

William J. Daugherty holds a doctorate in government from the Claremont Graduate School and is Associate Professor of government at Armstrong Atlantic State University in Savannah, Georgia. A retired senior officer in the CIA, he is also the author of *In the Shadow of the Ayatollah: A CIA Hostage in Iran* (Annapolis, 2001) and *Executive Secrets: Covert Action and the Presidency* (Kentucky, 2004).

Jack Davis served in the CIA from 1956 to 1990 as analyst, manager, and teacher of analysts. He now is an independent contractor with the Agency, specializing in analytic methodology. He is a frequent contributor to the journal *Studies in Intelligence*.

Stuart Farson is Lecturer, Political Science Department, Simon Fraser University, Vancouver/Surrey, Canada. He is a former Secretary-Treasurer of the Canadian Association for Security and Intelligence Studies, and served as Director of Research for the Special Committee of the House Commons (Canada) on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act. He has numerous articles on security, intelligence, and policing issues and is the coeditor of *Security and Intelligence in a Changing World* (with David Stafford and Wesley K. Wark, Cass, 1991).

Timothy Gibbs is a final-year doctoral student in history at Robinson College, Cambridge University, and a member of the Cambridge University Intelligence Seminar. He is also a former Visiting Scholar at the University of Georgia. His doctoral dissertation, titled *British and American Intelligence and the Atom Spies*, was submitted in the summer of 2006 and was supervised by Professor Christopher Andrew.

Peter Gill is Reader in Politics and Security, Liverpool John Moores University, Liverpool, United Kingdom. He is coauthor of *Introduction to Politics* (1988, 2nd ed.) and *Intelligence in an Insecure World* (2006). He is currently researching the control and oversight of domestic security in intelligence agencies.

Harold M. Greenberg graduated with a B.A. in history from Yale University in 2005. At Yale, he participated in the Studies in Grand Strategy program, and he has recently published research on CIA covert action in the 1950s. He now works as a legislative aide in the U.S. House of Representatives.

Daniel S. Gressang IV is Professor at the Joint Military Intelligence College (JMIC) in Washington, DC, and serves concurrently as the National Security Agency/National Cryptologic School of Liaison to JMIC. He has researched, written, and lectured extensively on terrorism and counterinsurgency. His research focuses primarily on the application of complex adaptive systems perspectives to understanding the dynamics of terror and other forms of unconventional warfare. In 2004, he was designated Intelligence Community Officer by the Director of Central Intelligence.

Glenn Hastedt received his doctorate in political science from Indiana University. Until recently he was Professor and Chair of the Political Science Department at James Madison University. He is now chair of the Justice Studies Department there. Among his publications is *American Foreign Policy: Past, Present, Future*, 6th ed. (Prentice Hall).

John Hollister Hedley, during more than thirty years at CIA, edited the *President's Daily Brief*, briefed the *PDB* at the White House, served as Managing Editor of the *National Intelligence Daily*, and was Chairman of the CIA's Publications Review Board. Now retired, Hedley has taught intelligence at Georgetown University and serves as a consultant to the National Intelligence Council and the Center for the Study of Intelligence.

Michael Herman served from 1952 to 1987 in Britain's Government Communications Headquarters, with secondments to the Cabinet Office and the Ministry of Defence. Since retirement he has written extensively on intelligence matters, with official clearance. He has had academic affiliations with Nuffield and St. Antony's Colleges in Oxford and is Founder Director of the Oxford Intelligence Group and Honorary Departmental Fellow at Aberystwyth University. In 2005 he received the degree of Honorary D.Litt from Nottingham University. He is a leading British intelligence scholar and author of *Intelligence Power in Peace and War* (Cambridge, 2001).

Frederick P. Hitz is Lecturer (Diplomat in Residence) in Public and International Affairs, Woodrow Wilson School, Princeton University.

Max M. Holland is the author of *The Kennedy Assassination Tapes* (Knopf, 2004).

Arthur S. Hulnick is Associate Professor of International Relations at Boston University. He is a veteran of thirty-five years of intelligence service, including seven years in Air Force Intelligence and twenty-eight years in the CIA. He is author of *Fixing the Spy Machine* (Praeger, 1999) and *Keeping Us Safe* (Praeger, 2004).

Rhodri Jeffreys-Jones is Professor of American History at the University of Edinburgh. The author of several books on intelligence history, he is currently completing a study of the FBI.

Ephraim Kahana is Professor of Political Science and faculty member in the Western Galilee College, Acre, Israel. He teaches courses on international relations, national security and intelligence, and foreign policy in the National Security Program in the University of Haifa. Kahana has written numerous papers on intelligence and foreign policy. His most recent book is the *Historical Dictionary of Israeli Intelligence* (2006).

Patrick Radden Keefe is a graduate of the School of Law at Yale University and is presently a Fellow with the Century Foundation in New York City. He is the author of *Chatter: Uncovering the Echelon Surveillance Network and the Secret World of Global Eavesdropping* (Random House, 2006), and has published essays in *The New York Review of Books*, *The New York Times Magazine*, the *New York Times*, the *Boston Globe*, the *Yale Journal of International Law*, *Legal Affairs*, *Slate*, and *Wired*. He has been a Marshall Scholar and a 2003 fellow at the Dorothy and Lewis B. Cullman Center for Scholars and Writers at the New York Public Library.

Jennifer D. Kibbe is Assistant Professor of Government at Franklin and Marshall College. Between 2002 and 2004, she was a postdoctoral fellow at the Brookings Institution. Her research interests include U.S. foreign policy, intelligence and covert action, presidential decision making, and political psychology. She has published work on U.S. policy in Iraq and the Middle East, and the military's involvement in covert actions.

Katharina von Knop is a doctoral candidate in Political Science at Leopold-Franzens University in Innsbruck, Austria, specializing in counter- and antiterrorism, and coeditor with Heinrich Neisser and Martin van Creveld of *Countering Modern Terrorism: History, Current Issues, and Future Threats* (2005).

Lawrence J. Lamanna is a doctoral candidate in the School of Public and International Affairs at the University of Georgia. He holds an M.A. from Yale University and a B.A. from the University of Notre Dame.

Ian Leigh is Professor of Law and Codirector of the Human Rights Centre at the University of Durham. He lives in Durham, England.

Kristin M. Lord is Associate Dean at George Washington University's Elliott School of International Affairs. In 2005–2006, she was a Council on Foreign Relations International Affairs Fellow and Special Adviser to the Under Secretary of State for Democracy and Global Affairs. Lord is the author of *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security Democracy or Peace* (SUNY Press, 2006); coeditor, with Bernard I. Finel, of *Power and Conflict in the Age of Transparency* (Palgrave Macmillan, 2000); and the author of numerous book chapters, articles, and papers on international politics and security. Lord received her doctorate in government from Georgetown University.

Minh A. Luong is Assistant Director of International Security Studies at Yale University, where he teaches in the Department of History. He also serves as adjunct Assistant Professor of Public Policy at the Taubman Center at Brown University.

Cynthia M. Nolan earned a doctorate at American University in the School of International Service, researching intelligence oversight. She is a former officer in the Directorate of Operations in the CIA and has published in the *International Journal of Intelligence and Counterintelligence*.

Kevin A. O'Brien is a former research associate with the Canadian Institute of Strategic Studies and is currently a senior analyst for RAND Europe.

Mark Phythian is Professor of International Security and Director of the History and Governance Research Institute at the University of Wolverhampton, United Kingdom. He is the author of *Intelligence in an Insecure World* (2006, with Peter Gill), *The Politics of British Arms Sales Since 1964* (2000), and *Arming Iraq* (1997), as well as numerous journal articles on intelligence and security issues.

Harry Howe Ransom is Professor Emeritus of Political Science at Vanderbilt University. He has a B.A. from Vanderbilt and an M.A. and Ph.D. from Princeton University. He was a Congressional Fellow of the American Political Science Association and a Fellow of the Woodrow Wilson International Center for Scholars. He taught at Princeton, Vassar College, Michigan State University, Harvard University, and the University of Leeds. His books include *Central Intelligence and National Security* (1958), *Can American Democracy Survive Cold War?* (1963), and *The Intelligence Establishment* (1970).

Jeffrey T. Richelson is Senior Fellow with the National Security Archive in Washington, DC, and author of *The Wizards of Langley*, *The U.S. Intelligence Community*, *A Century of Spies*, and *America's Eyes in Space*, as well as numerous articles on intelligence activities. He received his doctorate in political science from the University of Rochester and has taught at the University of Texas, Austin, and the American University, Washington, DC. He lives in Los Angeles.

Jerel A. Rosati is Professor of Political Science and International Studies at the University of South Carolina since 1982. His area of specialization is the theory and practice of foreign policy, focusing on the U.S. policy-making process, decision-making theory, and the political psychological study of human cognition. He is the author and editor of five books and over forty articles and chapters. He has received numerous outstanding teaching awards. He has been Visiting Professor at Somalia National University in Mogadishu and Visiting Scholar at China's Foreign Affairs College in Beijing. He also has been a Research Associate in the Foreign Affairs and National Defense Division of the Library of Congress's Congressional Research Service, President of the International

Studies Association's Foreign Policy Analysis Section, and President of the Southern region of the International Studies Association.

Richard L. Russell is Professor of national security studies at the National Defense University. He is also an adjunct associate professor in the Security Studies Program and research associate in the Institute for the Study of Diplomacy at Georgetown University. He previously served as a CIA political-military analyst. Russell is the author of *Weapons Proliferation and War in the Greater Middle East: Strategic Contest* (2005).

Frederick A. O. Schwarz Jr. received an A.B. from Harvard University and J.D. from Harvard Law School, where he was an editor of the *Law Review*. After a year's clerkship with Hon. J. Edward Lumbard, U.S. Court of Appeals for the Second Circuit, he worked one year for the Nigerian government as Assistant Commissioner for Law Revision under a Ford Foundation grant. He joined the New York City law firm of Cravath, Swaine and Moore in 1963 and was elected a partner in 1969. From 1975 through mid-1976, he served as Chief Counsel to the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the Church Committee); from 1982–89, he served as Corporation Counsel and head of the Law Department of the City of New York. In 1989, he chaired the New York City Charter Revision Commission.

James M. Scott is Professor and Chair of the Department of Political Science at Oklahoma State University. His areas of specialization include foreign policy analysis and international relations, with particular emphasis on U.S. foreign policy making and the domestic sources of foreign policy. He is author or editor of four books, over forty articles, book chapters, review essays, and other publications. He has been President of the Foreign Policy Analysis section and President of the Midwest region of the International Studies Association, where he has also served as conference organizer for both sections and has been a two-time winner of the Klingberg Award for Outstanding Faculty Paper at the ISA Midwest Annual Meeting. Since 1996, he has received over two dozen awards from students and peers for his outstanding teaching and research, including his institution's highest awards for scholarship in 2000 and 2001. Since 2005, he has been Director of the Democracy and World Politics Summer Research Program, a National Science Foundation Research Experience for Undergraduates.

Len Scott is Professor of International Politics at the University of Wales, Aberystwyth, where he is Director of the Centre for Intelligence and International Security Studies. Among his recent publications are *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows* (2004, coedited with Peter Jackson) and *Planning Armageddon: Britain, the United States and the Command of Nuclear Forces, 1943–1964* (2000, coedited with Stephen Twigge).

Katherine A. S. Sibley is Professor and Chair of the History Department at St. Joseph's University. She is currently working on a biography of Florence Kling

Harding, titled *America's First Feminist First Lady*. Sibley's work will revise the typical portrait of Mrs. Harding as manipulative, unhappy wife, casting new light on her public and private life. In 2004, Sibley published *Red Spies in America: Stolen Secrets and the Dawn of the Cold War* with the University Press of Kansas. She is also the author of *The Cold War* (1998) and *Loans and Legitimacy: The Evolution of Soviet-American Relations, 1919–1933* (1996). Her work has appeared in journals including *American Communist History*, *Peace and Change*, and *Diplomatic History*, and she also serves as book review editor for *Intelligence and National Security*. She is a three-term Commonwealth Speaker for the Pennsylvania Humanities Council.

Jennifer Sims is Director of Intelligence Studies and Visiting Professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service. She also consults for the U.S. government and private sector on homeland security and intelligence related matters. Prior to this, Sims was Research Professor at Johns Hopkins University's Nitze School of Advanced International Studies in Washington, DC (Fall 2001–Summer 2003). She has served as defense and foreign policy adviser to Senator John Danforth (1990–94), a professional staff member of the Senate Select Committee on Intelligence (1991–94), Deputy Assistant Secretary of State for Intelligence Coordination (1994–98), and as the Department of State's first Coordinator for Intelligence Resources and Planning in the office of the Under Secretary for Management. In 1998 Sims was awarded the U.S. Intelligence Community's Distinguished Service Medal. She received her B.A. degree from Oberlin College and her M.A. and Ph.D. in national security studies from Johns Hopkins University in 1978 and 1985, respectively. She is the author of a number of books and articles on intelligence and arms control. The most recent of these include "Foreign Intelligence Liaison: Devils, Deals and Details," *International Journal of Intelligence and Counterintelligence Affairs* (Summer 2006); *Transforming US Intelligence,* coedited with Burton Gerber (Georgetown University Press, 2005); "Transforming U.S. Espionage: A Contrarian's Approach," *Georgetown Journal of International Affairs* (Winter/Spring 2005); "Domestic Factors in Arms Control: The U.S. Case," in Jeffrey A Larson (ed.), *Arms Control: Cooperative Security in a Changing Environment* (Lynne Rienner, 2002); "What Is Intelligence? Information for Decision-Makers," in Roy Godson, Ernest R. May, and Gary Schmitt, *U.S. Intelligence at the Crossroads* (Brassey's, 1995); "The Cambridge Approach Reconsidered," *Daedalus* 120 (Winter 1991); and *Icarus Restrained: An Intellectual History of American Arms Control* (Westview Press, 1990).

Robert David Steele is CEO of OSS.Net, an international open source intelligence provider. As the son of an oilman, a Marine Corps infantry officer, and a clandestine intelligence case officer for the CIA, he has spent over twenty years abroad in Asia and Central and South America. As a civilian intelligence officer he spent three back-to-back tours overseas, including one tour as one of the first officers assigned full-time to terrorism, and three headquarters tours in offensive

counterintelligence, advanced information technology, and satellite program management. He resigned from the CIA in 1988 to be the senior civilian founder of the Marine Corps Intelligence Command. He resigned from the Marines in 1993. He is the author of three works on intelligence, as well as the editor of a book on peacekeeping intelligence. He has earned graduate degrees in international relations and public administration, is a graduate of the Naval War College, and has a certificate in Intelligence Policy. He is also a graduate of the Marine Corps Command and Staff Course and of the CIA's Mid-Career Course 101.

John D. Stempel is Senior Professor of International Relations at the University of Kentucky's Patterson School of Diplomacy and International Commerce, where he was Associate Director (1988–93) and Director (1993–2003). He came to the University of Kentucky following a 24-year career in the U.S. Foreign Service. There he focused on political and economic affairs, with overseas assignments in Africa (Guinea, Burundi, Zambia), Iran, and India, concluding with three years as U.S. Consul General in Madras. His Middle East service (1975–79) in Tehran provided the material for his book *Inside the Iranian Revolution*. His subsequent academic writings have focused on religion and diplomacy, intelligence and diplomacy, and American views of negotiation. His Washington assignments featured duty for both the State and Defense Departments, including a two-year tour as Director of the State Department's Crisis Center. He has taught at George Washington and American Universities, plus two years as Diplomat in Residence at the U.S. Naval Academy, Annapolis. Stemple is a member of the New York Council on Foreign Relations and is listed in *Who's Who in the World* and *Who's Who in America*. He holds an A.B. degree from Princeton University and M.A. and Ph.D. degrees from the University of California at Berkeley.

Stan A. Taylor is an Emeritus Professor of Political Science at Brigham Young University in Provo, Utah. He has taught in England, Wales, and New Zealand and in 2006 was a visiting professor at the University of Otago in Dunedin, New Zealand. He is founder of the David M. Kennedy Center for International Studies at Brigham Young University. He writes frequently on intelligence, national security, and U.S. foreign policy.

Athan Theoharis is Professor of History at Marquette University whose research has focused on government secrecy, Cold War politics, and the history of the FBI. He is the author, coauthor, and editor of eighteen books, including *The FBI and American Democracy* (2004), *Chasing Spies* (2002), *A Culture of Secrecy* (1998), and *The FBI: A Comprehensive Reference Guide* (1998). He has received numerous awards, including the American Bar Association's Gavel Award and selection as a fellow by the Wisconsin Academy of Arts, Sciences, and Letters.

Gregory F. Treverton is senior analyst at the RAND Corporation. Earlier, he directed RAND's Intelligence Policy Center and its International Security and Defense Policy Center, and he is Associate Dean of the Pardee RAND Graduate School. His recent work has examined at terrorism, intelligence, and law

enforcement, with a special interest in new forms of public-private partnership. He has served in government for the first Senate Select Committee on Intelligence, handling Europe for the National Security Council, and most recently as vice chair of the National Intelligence Council, overseeing the writing of America's National Intelligence Estimates. He holds an A.B. *summa cum laude* from Princeton University, a master's in public policy, and Ph.D. in economics and politics from Harvard University. His latest books are *Reshaping National Intelligence for an Age of Information* (Cambridge University Press, 2001), and *New Challenges, New Tools for Defense Decisionmaking* (edited, RAND, 2003).

Michael A. Turner is a political scientist who has taught international relations and national security matters in San Diego, California, for the past twelve years. Before that, he spent over fifteen years in various positions within the CIA. Turner is the author of *Why Secret Intelligence Fails* (2005; 2006) and the *Historical Dictionary of United States Intelligence* (2006).

Michael Warner serves as Historian for the Office of the Director of National Intelligence.

Nigel West is a military historian specializing in security and intelligence topics. He is the European editor of the *World Intelligence Review* and is on the faculty at the Center for Counterintelligence and Security Studies in Washington, DC. He is the author of more than two dozen works of nonfiction and recently edited *Guy Liddell Diaries*.

Reg Whitaker is Distinguished Research Professor Emeritus, York University, and Adjunct Professor of Political Science, University of Victoria, Canada. He has written extensively on Canadian and international security and intelligence issues.

James J. Wirtz is Professor in the Department of National Security Affairs at the Naval Postgraduate School, Monterey, California. He is Section Chair of the Intelligence Studies Section of the International Studies Association and President of the International Security and Arms Control Section of the American Political Science Association. Wirtz is the series editor for *Initiatives in Strategic Studies: Issues and Policies*, published by Palgrave Macmillan.

Amy B. Zegart is Associate Professor of Public Policy at the University of California, Los Angeles. A specialist on national and homeland security, she has served on the National Security Council staff, as a foreign policy advisor to the Bush-Cheney 2000 presidential campaign, and as a consultant to California state and local homeland security agencies. She has published articles in leading academic journals, including *International Security* and *Political Science Quarterly*, and is the author of *Flawed by Design: The Origins of the CIA, JCS, and NSC* (Stanford, 1999). She received her Ph.D. in political science from Stanford, where she studied under Condoleezza Rice, and an A.B. in East Asian Studies from Harvard University.

STRATEGIC INTELLIGENCE

STRATEGIC INTELLIGENCE

3

COVERT ACTION: BEHIND THE VEILS OF SECRET FOREIGN POLICY

Edited by
Loch K. Johnson

Intelligence and the Quest for Security

PRAEGER SECURITY INTERNATIONAL
Westport, Connecticut • London

Library of Congress Cataloging-in-Publication Data

Strategic intelligence / edited by Loch K. Johnson.
p. cm.—(Intelligence and the quest for security, ISSN 1932-3492)
Includes bibliographical references and index.
ISBN 0-275-98942-9 (set : alk. paper)—ISBN 0-275-98943-7 (vol. 1 : alk. paper)—
ISBN 0-275-98944-5 (vol. 2 : alk. paper)—ISBN 0-275-98945-3 (vol. 3 : alk. paper)—
ISBN 0-275-98946-1 (vol. 4 : alk. paper)—ISBN 0-275-98947-X (vol. 5 : alk. paper)
1. Military intelligence. 2. Intelligence service—Government policy. I. Johnson, Loch K., 1942–

UB250.S6385 2007
327.12—dc22 2006031165

British Library Cataloguing in Publication Data is available.

Library of Congress Catalog Card Number: 2006031165
ISBN: 0-275-98942-9 (set)
0-275-98943-7 (vol. 1)
0-275-98944-5 (vol. 2)
0-275-98945-3 (vol. 3)
0-275-98946-1 (vol. 4)
0-275-98947-X (vol. 5)
ISSN: 1932-3492

First published in 2007

Praeger Security International, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the Untied States of America

The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

CONTENTS

Appendixes

PREFACE

THIS FIVE-VOLUME SERIES IN INTELLIGENCE IS SOMETHING of a landmark in the study of intelligence. Thirty years ago, one would have been hard-pressed to find enough good articles on the subject to fill two volumes, let alone five. In those three decades since 1975, however, the study of intelligence has grown considerably. Today there are several solid professional journals in the field, including the premier publications *Intelligence and National Security* (published in the United Kingdom), *International Journal of Intelligence and Counterintelligence* (the United States), and *Studies in Intelligence* (from the Central Intelligence Agency, in both classified and unclassified form). In just the past two years, bulging anthologies on the general topic "strategic intelligence," as well as a "handbook" on intelligence and a collection of chapters within the more specialized niche of "intelligence and ethics" have appeared, along with a tidal wave of books and articles on one aspect or another of this subject (see the bibliographic essay in volume 1).

Except in times of scandal (Watergate in 1973, CIA domestic spying in 1974, the Iran-*contra* affair in 1987), one could find in this earlier era little newspaper coverage of intelligence activities, so tightly held were these operations by the government. Now, fueled by the events of the September 11, 2001, terrorist attacks and the erroneous prediction in 2002 that weapons of mass destruction (WMDs) were being developed and stockpiled by Iraq, hardly a week goes by without reports on intelligence in the *New York Times* and other leading newspapers. These days, the *Atlantic Monthly* and the *New Yorker*, America's top literary magazines, visit the subject with some regularity, too. The latter has hired Seymour M. Hersh, the nation's most well-known investigative reporter with an intelligence beat.

Intelligence studies has come of age.

Certainly the chapters in these volumes display a breadth of inquiry that suggests an admirable vibrancy in this relatively new field of study. Presented here are empirical inquiries, historical treatments, theoretical frameworks, memoirs, case studies, interviews, legal analyses, comparative essays, and ethical assessments. The authors come from the ranks of academe (twenty-five); the intelligence agencies (thirteen); think tanks (seven); Congress, the State Department, and the National Security Council (three); and the legal world (three).[1] Over a quarter of the contributors are from other nations, including Canada, England, Germany, Israel, Scotland, Switzerland, and Wales. The American writers come from every region of the United States. As a collective, the authors represent a wide range of scholarly disciplines, including computer science, history, international affairs, law, sociology, political science, public administration, public policy studies, and strategic studies. Many of the contributors are from the ranks of the top intelligence scholars in the world; a few young ones stand at the gateway to their academic careers.

Notable, too, is the number of women who have entered this field of study. Thirty years ago, it would have been rare to find one or two women writing on this subject. Seven have contributed chapters to these pages, and another two wrote documents that appear in the appendixes. This is still fewer than one would like, especially in light of the major contribution women have made as intelligence officers. One thinks of the heroic efforts of British women in code breaking and in the Special Operations Executive during World War II, and the American women who contributed so much to the analytic efforts of the Office of Strategic Studies (OSS) during that same war. At least, though, the number attracted to the scholar study of intelligence appears to be rapidly expanding.

The end result of this mix is a landscape illuminated by a variety of methods and appreciations—a rich research trove that examines all the key aspects of intelligence. In addition, each of the volumes contains backup materials in the appendixes. These documents provide the reader with access to significant primary and secondary sources referred to in the chapters.

The volumes are organized according to the major topics of studies in the field. The first volume, titled *Understanding the Hidden Side of Government*, introduces the reader to methods commonly used in the study of intelligence. It imparts, as well, a sense of the "state of the discipline," beginning with a bibliographic essay (by the editor) and continuing with an examination of specific approaches scholars have adopted in their inquiries into this especially difficult discipline, where doors are often shut against outsiders.

In the bibliographic essay that opens the volume, I argue that the literature on intelligence has mushroomed over the past thirty years. Some of this literature is unreliable, but much of it is of high quality. Amy B. Zegart follows my chapter with an important caveat: the literature may be more voluminous these days, but intelligence studies as an academic field has yet to be accepted as a vital part of national security scholarship. The mainstream journals of history, international

affairs, and political science have still regarded the study of intelligence as a marginal pursuit. In this regard, Zegart points out, there is a major disconnect between academic scholarship and those who make decisions in Washington, London, and other capitals around the world.

Following this introduction, Len Scott and Timothy Gibbs look at methods that have been used to study intelligence in the United Kingdom; Stuart Farson and Reg Whitaker in Canada; and Michael Warner in the United States. The volume then turns to a more specific inquiry into the central question of how intelligence is interpreted by professionals—the issue of analysis—explored by John Hollister Hedley. An overview of the sometimes turbulent relationship between intelligence officers and the policy makers they serve is explored by James J. Wirtz; and British scholar Peter Gill recalls the failures associated with the 9/11 attacks and the poor judgments about Iraqi WMDs, in hopes of extracting lessons from these intelligence disasters. In the next chapter, the youngest scholar represented in this collection, Harold M. Greenberg, takes us back in time with a remembrance of the legendary CIA officer and Yale history professor Sherman Kent, often known as the dean of CIA analysts. Kristin Lord rounds out the first volume with a look forward into future prospects for a more transparent world—the ultimate goal of intelligence.

As with each of the books, Volume 1 has a set of appendixes designed to supplement the original chapters with supportive materials from government documents and other sources. Appendix A contains the relevant intelligence excerpts from the National Security Act of 1947—the founding charter for the modern American intelligence establishment. Appendix B provides a history of U.S. intelligence since 1947, prepared for the Aspin-Brown Commission in 1995–96 by staff member Phyllis Provost McNeil. These two documents present a contextual backdrop for the Volume 1 chapters. Appendix C provides "wiring diagrams" of the intelligence community, that is, organizational blueprints for the sixteen agencies and related entities. One chart displays the community as it is today, and another displays how it looked in 1985. As the contrast between the two illustrates, the events of September 11, 2001, have led to a larger and more complex intelligence apparatus in the United States. Appendix D shows a photograph of the CIA Headquarters Building, as an example of what one of the secret agencies actually looks like from an aerial perspective. The white dome in the foreground is an assembly hall seating around 600 people and to its left is the main entrance to the original CIA headquarters, built during the Eisenhower years. Behind this older wing is the new green-glass structure erected during the Reagan administration, often known as the Casey addition because William J. Casey was the Director of Central Intelligence (DCI) at the time of its construction during the 1980s.

Appendix E lists the top leadership in the America's intelligence community: the DCIs from 1947–2005 and today's DNI. Included here as well are the leaders in Congress who have been responsible for intelligence accountability in the past, along with the current members of the two congressional Intelligence

Committees: the Senate Select Committee on Intelligence (SSCI, or "sissy" in the unflattering and sometimes true homophone of Capitol Hill vernacular) and the House Permanent Select Committee on Intelligence (HPSCI or "hipsee"). Appendix F presents a 1955 statement from historian and CIA analyst Sherman Kent about the need for a more robust intelligence literature. He would probably be amazed by how much is being written on this subject now. Appendix G offers an overview on the purpose and challenges of intelligence, drawn from the introductory chapters of the Aspin-Brown Commission Report. Finally, Appendix H provides an opening glimpse into the subject of counterintelligence, a world of counterspies and betrayal taken up more fully in Volume 4.

With the second volume, titled *The Intelligence Cycle: The Flow of Secret Information From Overseas to the Highest Councils of Government*, the focus shifts from a broad overview of intelligence to a more detailed examination of its core mission: the collection, analysis, and dissemination of information from around the world. The National Security Act of 1947, which created America's modern intelligence establishment, made it clear that the collection, analysis, and dissemination of information would be the primary duty of the intelligence agencies. As Allen Dulles—the most famous DCI (America's top intelligence official, until this title changed to director of National Intelligence or DNI in 2005)—put it, the intelligence agencies were expected "to weigh facts, and to draw conclusions from those facts, without having either the facts or the conclusions warped by the inevitable and even proper prejudices of the men whose duty it is to determine policy."[2] The collection and interpretation of information, through espionage and from the public record, would be the primary responsibility of America's secret agencies.

At the heart of this mission lies the so-called intelligence cycle. Professional intelligence officers define the cycle as "the process by which information is acquired, converted into intelligence, and made available to policymakers."[3] The cycle has five phases: planning and direction, collection, processing, production and analysis, and dissemination (see Appendix A in Volume 2 for a depiction). As former CIA officer Arthur S. Hulnick notes, however, in the opening chapter, the idea of a "cycle" fails to capture the complexity of how intelligence is collected, assessed, and distributed by intelligence officers.

The next five chapters in Volume 2 take us into the world of the "ints," that is, the specialized "intelligences" (methods) used by intelligence officers to collect information. Patrick Radden Keefe and Matthew M. Aid probe the method of signals intelligence or SIGINT, a generic term used to describe the interception and analysis of communications intelligence and other electronic emissions, from wiretapping telephones to studying the particles emitted by missiles in test flights. Both authors are sensitive to the possible abuse of these techniques, which can be and have been used to spy on Americans without a proper judicial warrant. Jeffrey T. Richelson explores the IMINT domain, that is, imagery intelligence or, in simple terms, photographs taken by surveillance satellites and reconnaissance airplanes (piloted and unpiloted). Telephone conversations can be revealing, but

in the old saying, a picture can be worth a thousand words. (Appendix B provides photographic examples of these spy platforms, and Appendix C offers illustrations of the IMINT data they can collect.)

Important, too, is information that can be acquired by human agents ("assets") guided by case officers inside the CIA or the Defense Department, the topic of human intelligence or HUMINT, examined by Frederick P. Hitz. Not all the information needed by policy makers is acquired through SIGINT, IMINT, or HUMINT; indeed, the overwhelming majority—upward of 95 percent—is already in the public domain. This open-source intelligence (OSINT) must be sorted through, organized, and integrated with the secretly gained information. Robert David Steele's chapter looks at OSINT and its ties to the other ints.

In the next chapter, Daniel S. Gressang IV dissects some of the technological challenges faced by intelligence agencies in sorting through the avalanche of data that pours into their headquarters from various intelligence collectors around the world. Here is the Herculean task of sorting out the wheat from the chaff (or the signal from the noise, in another widely used metaphor) in the search for information that may warn the nation of impending peril. Here is the vital task of providing "indicators and warnings" (I&W) to a nation's leaders.

One of the most difficult relationships in the complex process of collection, analysis, and dissemination of information comes at the intersection between intelligence professionals and policy makers—groups of individuals that often have very different training, aspirations, and cultures. Jack Davis sheds light on this often turbulent relationship in the United States, and Michael Herman tackles the same topic in the United Kingdom. Minh A. Luong offers a case study on economic intelligence that underscores some of the difficulties encountered as information travels from the collectors and analysts (the "producers" of intelligence) to the policy makers (the "consumers"). Finally, Max M. Holland takes a look at how intelligence agencies examine their own mistakes ("postmortems") and attempt to make corrections—and how political consideration enter into the process.

By way of supporting documentation, in addition to the appendixes already mentioned, Appendix D outlines the general types of reports prepared by the producers of intelligence, along with a listing of specific examples. Appendixes E and F provide samples of key intelligence products: National Intelligence Estimates (NIEs)—the most important long-range and in-depth forecasting carried out by the U.S. secret agencies ("research intelligence," in contrast to shorter intelligence reports that tend to focus on near-term events, or "current intelligence"); Special National Intelligence Estimates (SNIEs), which concentrate on a narrow, high-priority information requirement (say, the capabilities of the Chinese military); and the *President's Daily Brief* (PDB), the most exclusive current intelligence report prepared by the intelligence agencies for the consumption of the president and a few other high-ranking officials.

In light of the fact that every study of the 9/11 and Iraqi WMD intelligence failures find fault, in part, with America's capacity for human intelligence—

especially in the Middle East and Southwest Asia—Appendix G presents one of the most searing critiques of this int. The critique, by the House Permanent Select Committee on Intelligence, has become all the more significant because the panel's chairman, Representative Porter Goss (R-FL), soon after the completion of the report rose to the position of the DCI. Last, Appendix H provides an excerpt from a key report on the Iraqi WMD mistakes, prepared by the "Roberts Committee": the Senate Select Committee on Intelligence, led by Pat Roberts (R-KS).

The third volume, titled *Covert Action: Behind the Veils of Secret Foreign Policy*, enters an especially controversial compartment of intelligence: the means by which the United States attempts to not just gather and analyze information about the world—hard enough—but to manipulate global events through secret activities in the advancement of America's best interests. An ambiguous passage of the National Security Act of 1947 charged the National Security Council (NSC), the boss over the sixteen U.S. secret agencies, to "perform such other functions and duties related to intelligence [over and beyond collection-and-analysis] affecting the national security as the National Security Council may from time to time direct."[4] The phrase "other functions and duties" left the door open for launching the CIA (and more recently the Pentagon) on a wide range of covert actions around the world.

Covert action (CA), sometimes referred to as the "quiet option," is based on the supposition that this secret approach to foreign affairs is likely to be less noisy and obtrusive than sending in the Marines. Sometimes professional practitioners also refer to covert action as the "third option," between diplomacy and open warfare. As former Secretary of State and National Security Adviser Henry Kissinger once put it: "We need an intelligence community that, in certain complicated situations, can defend the American national interest in the gray areas where military operations are not suitable and diplomacy cannot operation."[5] Still others prefer the euphemism "special activities" to describe covert action. Whatever the variation in terminology, the goal of covert action remains constant: to influence events overseas secretly and in support of American foreign policy.

Covert action operations are often grouped according to four broad categories: propaganda, political, economic, and paramilitary (PM) activities. An example of a propaganda operation was the CIA's use of Radio Free Europe during the Cold War to transmit anti-communist themes into nations behind the Iron Curtain. A political CA during the Cold War was the CIA's clandestine funneling of funds to the anti-communist Christian Democratic Party in Italy. An economic example: the CIA attempted to destroy electric power stations in Nicaragua during the 1980s, as a means of undermining the Marxist-oriented S*andinista* regime. PM operations can including everything from assassination plots against foreign heads of state to arming and guiding pro-American insurgent armies in one country or another. Little wonder this has been a controversial subject.

Gregory F. Treverton introduces the reader to covert action in the first chapter of Volume 3. He is followed by Kevin A. O'Brien and Ephraim Kahana, who discuss the use of covert action by other nations. The next four chapters illuminate certain aspects of CA, with James M. Scott and Jerel A. Rosati providing an overview of CA tradecraft (that is, the tools used to implement such operations); Michael A. Turner evaluating the merits of CIA covert propaganda operations; William J. Daugherty looking at political and economic examples of covert action; Jennifer D. Kibbe exploring the entry of the Defense Department into this domain; and former diplomat John D. Stempel contrasting the uses of covert action to diplomatic initiatives. Winding up the volume is Judge James E. Baker's legal analysis of covert action.

Supporting documents include excerpts from the Church Committee Report on the evolution of covert action as carried out by the CIA (Appendix A). The supervision of covert action went from an informal to a highly formal process, as a result of a law known as the Hughes-Ryan Act, passed on December 31, 1974. The language of this statute is presented in Appendix B, and the covert action procedures that resulted from the law are outlined in Appendix C. At the center of the covert action decision process since the Hughes-Ryan Act is the *finding*, a term of art that stems from the passage in the law that requires the president to "find" that a particular covert action proposal is important and has the president's approval. Appendix D contains two findings from the Iran-*contra* era in the mid-1980s. Covert actions must have an organizational apparatus to carry them out, and Appendix E displays what that apparatus looked like during the Cold War (and in basic form remains the organizational chart today, with a few name changes in the boxes).

One of the most controversial forms of covert action has been the assassination of foreign leaders. Appendix F presents a case study from the Church Committee on the CIA assassination plot hatched against the leader of the Republic of Congo, Patrice Lumumba, in 1960. The Committee's exposé of this and other plots led President Gerald R. Ford to sign an executive order prohibiting assassination as an instrument of American foreign policy (see Appendix G). The executive order has been waived in times of authorized warfare against other nations, however, leading to failed attempts to assassinate Saddam Hussein in the first and second Persian Gulf Wars (he was eventually captured alive in 2004, hidden away in a hole near his hometown in Iraq) and Al Qaeda leader Osama bin Laden during the Clinton administration. Considerable ambiguity exists regarding the current status of the executive order and under what conditions it might be waived by administrations. Finally, Appendix H—drawing on a presidential commission study and congressional hearings—examines covert action at its lowest state: the Iran-*contra* affair of the 1980s, when this approach to foreign policy subverted the U.S. Constitution and several laws (including the Hughes-Ryan Act).

A third intelligence mission, after collection-and-analysis and covert action, is counterintelligence (CI) and its associated activity, counterterrorism (CT).

Here is the concentration in Volume 4, titled *Counterintelligence and Counterterrorism: Defending the Nation Against Hostile Forces*. Like covert action, CI went without specific mention in the National Security Act of 1947. By the early 1950s, however, it had similarly achieved a status of considerable importance as an intelligence mission. CI specialists soon waged nothing less than a secret war against antagonistic intelligence services (especially the Soviet KGB); and, after the Cold War, CT specialists would focus on efforts to block terrorists who targeted the United States and its allies. Explaining why the mission of counterintelligence/counterterrorism evolved, a CI expert has pointed out that "in the absence of an effective U.S. counterintelligence program, [adversaries of democracy] function in what is largely a benign environment."[6]

The practice of counterintelligence consists of two matching halves: security and counterespionage. Security is the passive or defensive side of CI, involving such devices as background investigations, fences, sentries, alarms, badges, watchdogs, and polygraphs (lie detection machines). Counterespionage (CE) is the offensive or aggressive side of CI. The most effective CE operation is the infiltration of an American agent or "mole" into the enemy camp, whether a hostile intelligence service or a terrorist cell—a ploy called a penetration. Thus, the practice of security is, according to one of America's top counterintelligence experts, "All that concerns perimeter defense, badges, knowing everything you have to know about your own people," whereas the CE side "involves knowing all about intelligence services—hostile intelligence services: their people, their installations, their methods, and their operations."[7]

Stan A. Taylor and Nigel West clarify these issues in the first two chapters of this volume, then in the next two chapters Katherine A. S. Sibley and Athan Theoharis examine the challenges of keeping the United States spy-free. Rhodri Jeffreys-Jones looks at the efforts in Europe to create a counterintelligence capability similar to that practiced by America's Federal Bureau of Investigation (FBI). Glenn Hastedt takes the reader into the counterterrorism thicket in Washington, DC, explaining how politics influences CI and CT operations. Richard L. Russell and Jennifer Sims discuss the ups and downs of trying to establish an effective counterterrorism response in the United States, complicated by the fragmentation of authority and widely differing cultures among the sixteen U.S. intelligence agencies. Finally, Katharina von Knop looks at the rising role of women in terrorist organizations.

The back-of-the-book documents in Volume 4 begin with a look at the Church Committee findings regarding counterintelligence in 1975 (Appendix A), followed by the notorious Huston Plan—a master counterintelligence spy plan drafted by White House aide Tom Charles Huston in 1970, in response to a nation at unrest over the war in Vietnam (Appendix B). The Huston Plan is a classic illustration of overreaction in a time of domestic strife. In Appendix C, the Senate Select Committee on Intelligence summarizes its findings about the Aldrich H. Ames counterintelligence disaster. Next the appendixes include a series of U.S. commission conclusions about how to improve intelligence in the struggle

against global terrorism, whether locating and penetrating their cells in advance of a terrorist attack or thwarting the ability of terrorists to acquire WMDs. The panel reports include: the Hart-Rudman Commission of 2001 (Appendix D); the 9/11 or Kean Commission of 2004 (Appendix E); and the Silberman-Robb Commission of 2005 (Appendix F). For purposes of comparison, the final appendix (G) examines the conclusions reached by a British commission that also probed the Iraqi WMD failure: the Butler Report of 2004.

The fifth volume in the series, titled *Intelligence and Accountability: Safeguards Against the Abuse of Secret Power*, stems from a concern that secret power might be misused by those in high office. This danger was underscored in 1975 when Congress found the U.S. intelligence agencies guilty of spying against law-abiding American citizens, and again in 1987 during the Iran-*contra* affair when some elements of the intelligence community violated the public trust by ignoring intelligence laws. The United States has been one of the few nations in the world to conduct an ongoing experiment in bringing democratic accountability to secret government activities. Democracy and spying don't mix well. Secrecy runs counter to democratic openness, while at the same time openness possesses a threat to the success of espionage operations. Democracies need intelligence agencies to acquire information that may protect them, but thoughtful citizens worry about having secret agencies in an open society.

Until 1975, the nation's remedy for the tension between intelligence gathering and democracy was to trust the intelligence agencies and hope for the best. Elected officials treated the secret services as exceptional organizations, immune from the checks and balances envisioned by the framers of the Constitution. Lawmakers were satisfied with this arrangement, because if an operation went awry they could duck responsibility. When James R. Schlesinger, DCI in 1973, attempted to inform John Stennis (D-MS), a key member of the Senate Armed Services Committee, about an approaching operation, the Senator stopped him short: "No, no, my boy, don't tell me. Just go ahead and do it, but I don't want to know."[8]

This attitude on Capitol Hill—overlook rather than oversight—underwent a dramatic turnabout in December 1974, however, when the *New York Times* reported on allegations of CIA spying at home and questionable covert actions in Chile. Congress might have waved aside the revelations about Chile as just another Cold War necessity in the struggle against regimes leaning toward Moscow, but spying on American citizens—voters—was another matter altogether. In January 1975, President Ford created the Commission on CIA Activities Within the United States (the Rockefeller Commission, led by his vice president, Nelson Rockefeller). Later that month the Senate established a select committee to investigate intelligence activities. The committee was headed by Frank Church, D-ID, and became known as the Church Committee (the editor served as Church's assistant). A counterpart House committee, led by Representative Otis Pike (D-NY), began investigations the following month.

These various panels, especially the Church Committee, found many more improprieties than they had expected. Not only had the CIA engaged in domestic

spying in violation of its charter, so had the FBI and several military intelligence units. Furthermore, the FBI had carried out secret operations, known collectively as COINTELPRO, against thousands of civil rights activists, members of the Ku Klux Klan, and Vietnam War dissenters. The objective was to make their lives miserable by disrupting their marriages and employment. The Bureau even attempted to blackmail Dr. Martin Luther King Jr. into committing suicide. Church Committee investigators also discovered CIA assassination plots against foreign leaders and efforts to topple President Salvador Allende of Chile, even though he had been democratically elected.

These revelations convinced lawmakers that the time had come to bring accountability into the dark recesses of government. Congress established intelligence oversight committees in both chambers—the Senate in 1976 and the House a year later—and, by 1980, required by law timely reports on all secret intelligence operations. The new Committees pored over intelligence budgets, held regular hearings (mostly in closed session to protect spy sources and methods) and seriously examined the performance of America's intelligence agencies. No other nation has ever so thoroughly applied democratic principles to its secret services, although a number are now beginning to follow the leadership of the United States toward greater intelligence supervision.[9]

Since 1975, this effort has evolved in fits and starts. Sometimes lawmakers have insisted on close accountability, as when they enacted the Intelligence Oversight Act of 1980 with its stringent reporting requirements for covert operations, or when a series of laws in the 1980s sought to end covert actions in Nicaragua. At other times, members of Congress have loosened the reins—for example, repealing in 1985 a prohibition against covert action in Angola. On still other occasions, Congress has concentrated on helping the intelligence agencies improve their security and performance, as with a law in 1982 that prohibited exposing the names of undercover officers. The Iran-*contra* scandal of 1987 was a major setback to this new oversight, as the Reagan administration bypassed most of these rules and statutes in its conduct of a covert war in Nicaragua against the will of Congress. The scandal was an alert to lawmakers. The Intelligence Oversight Act of 1991 further tightened intelligence supervision by clarifying reporting requirements. Lawmakers also set up an Office of Inspector General in the CIA, confirmed by and accountable to Congress.

The pulling and tugging has continued, most recently over whether President George W. Bush violated the Foreign Intelligence Surveillance Act (FISA) of 1978 by conducting warrantless wiretaps as part of the war against terrorism in the aftermath of the 9/11 attacks. The FISA required warrants, but the White House claimed (when the secret operation leaked to the media) the law had become to cumbersome and, besides, the president had inherit authority to conduct the war against terrorism as he saw fit. This debate aside for the moment (several authors address the issue in these volumes), one thing is certain: the intelligence agencies in the United States are now very much a part of the nation's system of checks and balances. Americans want and deserve both civil liberties and a secure defense

against threats; so the search continues for an appropriate balance between liberty and security, democracy and effectiveness—precisely the topic of Volume 5.

The set of chapters on intelligence accountability are introduced with a chapter by David M. Barrett, the foremost authority on the history of accountability in the early years of modern U.S. intelligence (1947 to 1963). The chief counsel of the Church Committee, Frederick A. O. Schwarz Jr., then reflects back on the effects of that watershed inquiry. Next, the editor offers a previously unpublished interview with DCI William E. Colby, who stood at the helm of the intelligence community as it weathered the storm of the investigations into domestic spying during 1975. Mark Phythian presents a chapter on the British experience with intelligence accountability; and, comparing British and American oversight, Lawrence J. Lamanna contrasts the responses on both sides of the Atlantic to the faulty Iraqi WMD assessments in 2002.

The next chapter, written by Cynthia M. Nolan, looks at contemporary issues of intelligence oversight in the United States. Hans Born and Ian Leigh follow with a comparative dimension by contrasting intelligence accountability practices in a variety other nations. Finally, A. Denis Clift and Harry Howe Ransom, who have witnessed the unfolding of intelligence accountability over the past four decades, offer their appraisals of where the experiment stands today.

The first supporting document in this volume is a succinct legislative history of intelligence accountability from 1947 to 1993, prepared by the Senate Select Committee on Intelligence (Appendix A). Then come a series of important oversight laws, beginning with FISA in 1978. With this law, members of Congress sought to rein in the open-ended authority of the executive branch to wiretap and otherwise spy on individuals considered risks to the national security—a privilege abused by a number of administrations from the 1930s forward. Henceforth, FISA required a warrant from a special court (the FISA Court, whose members are appointed by the Chief Justice of the Supreme Court) before such intrusive measures could be carried out. This law, a hot topic in 2005–6 when critics charged the second Bush administration with violation of the warrant requirement, can be found in Appendix B.

The Intelligence Oversight Act of 1980 is presented in Appendix C. This is a brief but nonetheless far-reaching law, enacted by Congress as an attempt to become an equal partner with the executive branch when it came to intelligence. The 1991 Intelligence Oversight Act (Appendix D) emerged after the Iran-*contra* scandal and provided a tightening and clarification of the language in its 1980 precursor, especially with respect to the approval and reporting rules for covert action. The political tug-of-war over the drafting of this currently prevailing oversight statute was intense, leading to the first and only presidential veto of an intelligence act. President George H. W. Bush found the proposal's insistence on prior reporting of covert action objectionable in times of emergency. Lawmakers entered into a compromise with the chief executive, settling on a two-day reporting delay in emergencies. The bill passed Congress again, this time without a presidential veto.

In 1995, the House Permanent Select Committee on Intelligence launched an inquiry into a wide assortment of intelligence issues, stimulated initially by counterintelligence concerns (Aldrich Ames's treasonous activities at the CIA had recently been discovered) but turning into an opportunity for a broad review of new challenges that faced the secret agencies now that the Cold War had ended. In Appendix E, an excerpt from the Committee's final report examines the state of intelligence accountability in the mid-1990s. The next document, in Appendix F, carries the examination into the twenty-first century, with the appraisal of the 9/11 Commission on the same subject. The commissioners were unimpressed, referring to intelligence accountability as "dysfunctional."

At the center of any efforts to maintain accountability for the secret agencies lies the question of funding—the mighty power of the pursue, held in the hands of lawmakers. Appendix G draws on the findings of the Aspin-Brown Commission to provide official documentation about how the United States spends money for spying. Finally, in Appendix H, DCI Robert M. Gates (1991–93) offers observations about oversight from the perspective of the intelligence community management team, located at that time on the Seventh Floor of the CIA.

Here, then, is what the reader will find in these five volumes. The editor and the contributors hope the chapters and documents will help educate the public about the importance of intelligence agencies, as well as stimulate scholars around the world to further the blossoming of this vital field of study. I am pleased to acknowledge my gratitude to Praeger's Heather Staines, senior project editor, and Anne Rehill, development editor, each a pleasure to work with and most helpful in their guidance; Julie Maynard at the University of Georgia for her administrative assistance; Lawrence J. Lamanna, my graduate research assistant, for his good counsel and logistical help; Leena S. Johnson for her indispensable encouragement and support; and the contributors to these volumes for their outstanding scholarship and their much appreciated cooperation in keeping the publishing train running on time.

These volumes are enthusiastically dedicated to Harry Howe Ransom, who has done so much in the United States to lead the way toward a serious discipline of intelligence studies.

Loch K. Johnson

NOTES

1. Some of the authors have had multiple careers, so in categorizing them I have counted the place where they have spent most of their professional lives.

2. Quoted by Senator Frank Church (D-ID), in *Congressional Record* (January 27, 1976), p. 1165.

3. *Fact Book on Intelligence* (Washington DC: CIA Office of Public Affairs, April 1983), p. 17.

4. National Security Act of 1947, signed on July 26, 1947 (P.L. 97-222; 50 U.S.C. 403, Sec. 102).

5. Comment, "Evening News," NBC (January 13, 1978).

6. Editor's interview with a FBI counterintelligence specialist, Washington, DC (May 16, 1975).

7. Editor's interview with Raymond Rocca, CIA/CI specialist, Washington, DC (November 23, 1975).

8. Editor's interview with James R. Schlesinger, Washington, DC (June 16, 1994).

9. See Hans Born, Loch K. Johnson, and Ian Leigh, *Who's Watching the Spies? Establishing Intelligence Service Accountability* (Washington, DC: Potomac Books, 2005).

1

COVERT ACTION

Forward to the Past?

GREGORY F. TREVERTON

MY INTRODUCTION TO COVERT ACTION WAS A fascinating one, moving as a graduate student and then freshly minted Ph.D. to Washington to work for the original Senate Select Committee on Intelligence—often called the Church Committee after its chair, Sen. Frank Church (D-ID).[1] The investigations, hard on the heels of Watergate and allegations of covert U.S. intervention in Chile, were the nation's first ever look behind the green wall of intelligence. I had written about presidential decision making and expected to work on the role of intelligence analysis in those decisions.

In fact, I spent virtually all my time on covert action, and much of that on Chile.[2] That stint in Washington was exhilarating and frustrating, and it produced one of very few "aha!" moments I've had researching in deeply classified documents. Press accounts had attributed to Henry Kissinger, then the National Security Advisor, the line: "I don't see why the United States should stand by and watch Chile go communist merely due to the stupidity of the Chilean people." The quote rang true enough, but I hadn't seen a source and didn't expect to. Then, we received a spate of highly classified documents, including minutes from the 40 Committee, the administration's interagency committee for reviewing covert actions.[3]

Kissinger, previously a scholar, had changed the committee's record keeping from the terse notations of previous administrations—"CIA project 123 is approved," with no mention of operation or country—to those of a recording secretary. So there it was at the end of the notes on one meeting: "The chairman [Kissinger] closed the meeting by observing that he didn't see why . . ."

When I reflected some years later on covert action, what struck me was how much the targets of U.S. covert action had changed from the 1940s to the 1990s.[4]

Many of the CIA's early postwar targets, like Iran's Mossadeq or Guatemala's Arbenz, wanted, almost pleadingly, not to be enemies of the United States. However, for later targets, like Nicaragua's Sandinistas or Iran's Khomeini, the United States was more useful as an enemy than a friend. Cuba's Castro bridged the two periods, with America-as-foe becoming the best thing he had going for him.

By the end of the 1990s, a second theme was also apparent: major American "secret" operations, from Nicaragua and Angola to Cambodia and Afghanistan, were not very secret. They had become "overt" covert action, in that actions became public not just when their results were known but while they were in progress. Support for the Nicaraguan rebels, or contras, the most controversial example, was openly debated and openly funded. Neither opponents nor supporters had reason to keep it secret; for its part the Reagan administration regarded covert action as good policy and good domestic politics, a key element of the Reagan Doctrine, which was intended to challenge Marxist-Leninist states around the world. Indeed, when the Reagan administration decided to sell arms to Iran and keep the operation secret, it turned inward, to the White House staff.[5] In embroidering that operation to divert money for the contras, White House aides apparently kept the president ignorant to protect him—providing him with plausible denial of the sort the CIA had long since abandoned.

Now, the United States has come full circle. Not only are most covert actions not very secret, they are mostly paramilitary actions in support of broader, mostly military counterterrorism operations. The campaign against terror has thrown CIA covert operators and Pentagon special forces together in new ways. The successes of that cooperation, in Afghanistan and Iraq, have been impressive. Because the operations are not very secret and because they are part of the broader campaign against a fearsome foe—transnational terrorism—the questions of how to square them with America's values are less evident. Yet the process is making for less clarity about who does what and why. More important, it is complicating who *authorizes* lethal force and on what basis.

This chapter first reviews the early history that set the pattern for U.S. covert action in the half a century after World War II and inquires into how the success or failure of covert actions should be judged. It then looks at the circumstances, both at home and abroad, that changed covert action to "overt covert," and it argues for a bias toward acting openly, not covertly. If covert action is to be employed, what lessons emerge from the history? It then asks how those lessons apply in current circumstances, and it concludes with a coda on how the oversight of intelligence, especially covert action, by Congress has functioned.

EARLY SUCCESSES SET THE PATTERN

Spying may be the world's second oldest profession, but for the United States it was only the Cold War, coming on the heels of America's wartime experience with secret operations conducted by the Office of Strategic Services,

that led to the creation of an intelligence service in peacetime and to covert operations. Notice that spying—human intelligence or HUMINT, in the jargon of the trade—and covert action are superficially similar but in fact quite different. Both involve secret relationships between U.S. intelligence officers and foreigners. But the point of spying is information; the U.S. officer is relatively passive and the process is designed to protect the foreign spy's link to the United States. For covert action, by contrast, the purpose is doing something; the U.S. officer is active and the process carries inherent risks of being blown—the riskier it is, the more ambitious the action.

Wartime success and postwar threat: these were the backdrop for the creation of the Central Intelligence Agency (CIA). In a few years America plunged from the euphoria of victory in World War I1 to the confrontation with a looming Soviet threat, when Western Europe seemed to teeter in the balance. The first line of American response to the onset of the Cold War was overt: the surge of assistance to Europe through the Truman Doctrine and the Marshall Plan. But the second line was renewed interest in what was then called covert psychological warfare—what we could now call propaganda—as a way to respond to the Soviet Union by means that were less than war but more than nothing.

In this atmosphere, the National Security Council approved NSC 1012, a plan that had originated with George Kennan, then director of the State Department's Policy Planning Staff and the author of the famous X article outlining the policy of containment of the Soviet Union. NSC 1012 was the turning point for covert action, expanding it from propaganda to direct intervention. In the words of the document, covert action comprised: "propaganda, economic warfare; preventive direct action, including sabotage, anti-sabotage, demolition and evacuation measures; subversion against hostile states, including assistance to underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anticommunist elements."[6] NSC 1012 also codified the notion of plausible denial: operations were to be "so planned and executed that any U.S. Government responsibility for them is not evident to unauthorized persons and that if uncovered the U.S. Government can plausibly disclaim any responsibility for them."

The fledgling CIA's first success came that same year, in 1948, when its covert support to the Italian Christian Democrats helped them beat back an electoral challenge from the Italian Communist Party. By 1950 the United States had succeeded in the covert struggle in Western Europe; in Eastern Europe its covert operations wound down to propaganda and intelligence gathering. The center of the battle against communism moved, as Washington saw the world, away from Europe to small, weak countries. Europe had put the CIA into the business of covert political action, but Asia got the agency into secret paramilitary operations in the Korean War, a pattern repeated a decade later in another Asian war, Vietnam.

The incoming Eisenhower administration called for a more active response to the Soviet threat than the passive containment of the Truman administration.

CIA operators soon registered two successes that set the pattern for the next two decades. On August 21, 1953, after a week of turmoil in the streets of Tehran, the Iranian prime minister, Mohammed Mossadeq, who had nationalized that country's oil industry, surrendered. Three days later the shah, who had fled Iran the previous week with his queen, returned to the capital. At his palace a few days later, he offered a toast to Kermit "Kim" Roosevelt, the chief of the CIA's Near East and Africa Division and the man who had improvised Mossadeq's downfall: "I owe my throne to God, my people, my army—and you!"[7]

The next year, on June 16, 1954, Guatemalan Colonel Carlos Castillo Armas crossed the border into his country from Honduras with a few hundred men trained and armed by the CIA. Pilots under CIA contract flew air cover. The president of Guatemala, Jacobo Arbenz Guzmán, was deserted by his air force and his army, which refused his order to arm workers and peasants. The American ambassador hastily arranged a transfer of power to the chief of the armed forces. (In a moment of tragicomedy, that man immediately pledged that he would continue the struggle against Castillo Armas, America's designated successor to Arbenz. Only after complicated negotiations led by the ambassador did Castillo Armas emerge as president.)[8]

The Iran and Guatemala operations—code-named TPAJAX and PBSUCCESS, respectively—coming within a few years of the CIA's success in Western Europe, made the agency's reputation and set the pattern for covert action in the years ahead. Small, cheap, fast, and tolerably secret, they encouraged Washington to think other covert actions could be likewise. When the next administration decided to confront revolution in Cuba, its covert response was the same as in Guatemala. So were the CIA officers who carried it out.

The blush of short-run success amidst the Cold War obscured several warnings. In the early 1950s, both Iran and Guatemala were eminently vulnerable to manipulation by an outside power, particularly the United States. In both, contending political forces were in close balance. Those balances might have tipped against Mossadeq and Arbenz even if the CIA had not intervened. So it appeared that relatively small operations were enough to tip the balance. Yet in both cases, limited interventions might have failed. In fact, Kermit Roosevelt's first plot did fail; CIA Director Allen Dulles was ready to roll up the operation and bring the troops home. And the CIA officers who ran PBSUCCESS were under no illusions: if their deceptions failed and Arbenz were able to get his military into combat, the invaders would be overwhelmed.

Thus, success was purchased at the price of enlarging the intervention. American purposes did not change, but the operational requirements of achieving them did. Once the United States was committed, in secret and in a small way, the stakes increased, and the CIA took the next step. The effort to intimidate Arbenz became a paramilitary campaign, if a small one. In the process, plausible deniability became more tenuous.

Six years later at the Bay of Pigs, deniability evaporated entirely. "How could I have been so stupid, to let them go ahead?"[9] The words were from John

Kennedy. When the CIA trained invasion force of Cuban exiles hit the beach in the early dawn hours of April 17, 1961, everything went wrong: the lives of brave Cubans were spent; the United States was seen to be intervening; and the intervention failed. Once the plan had changed (without anyone outside the CIA quite noticing it) from a guerrilla operation into a full-fledged amphibious invasion, the chance of keeping it tolerably secret diminished to the vanishing point.

JUDGING SUCCESS

Evaluating covert action in retrospect is speculative, for it is bedeviled by the imponderable of what might have been; history permits no reruns. Failures, such as the Bay of Pigs invasion, are apparent, but successes are harder to judge. Consider the CIA intervention in the Angolan civil war of 1975. On the surface it was a failure: the Cuban- and Soviet-supported faction, the MPLA (Popular Movement for the Liberation of Angola), was installed while the U.S. role in trying to prevent that outcome was being exposed. If, however, the initial purpose was more limited—for instance, to raise the price of victory for the MPLA and its Soviet and Cuban backers—then Angola might be counted a short-run success. Yet American officials did not convey the impression that their aims actually were so limited, either at the time or later.

When, on the one hand, covert actions have succeeded in their short-run purposes, it may be that the action, though marginal, was just the bit of "support for our friends" that tipped the balance in the internal politics of a foreign country. On the other hand, it may be that the American support was entirely superfluous, and the same successful outcome would have ensued without the U.S. involvement. If this is so, all the covert action accomplished was to implicate the United States and tarnish the success by labeling it "made in America" when the existence of the covert action became known.

A case in point was covert American support to opposition political parties and media in Chile during the presidential tenure of Salvador Allende (1970–73), a self-proclaimed Marxist. There is no question that those parties and media were under pressure from the Allende government.[10] The opposition forces survived to fight another day, but there is no telling whether CIA support for them was decisive or irrelevant.

What is clear is the signal conveyed to history by the revelations of American covert action. In retrospect, most reasonably objective observers conclude that Allende's experiment in Chile would have failed on its own terms.[11] Yet history's lesson is not that Allende fell of his own accord but that the United States overthrew him in 1973. That is the public perception, even though this lesson is untrue in the narrow sense: Washington did not engineer his coup, nor did the CIA or the American military participate in it. The very fact of American covert action meant that at a minimum, "it is fair to say that the United States cannot escape some responsibility for [Allende's] downfall."[12]

By the same token, in 1975 when South Africa intervened to back the U.S.-supported Angolan factions, the FNLA (National Front for the Liberation of Angola) and UNITA (National Union for the Total Independence of Angola), a covert action originally intended to counter the Soviet Union and Cuba, then signaled something else. It indicated an alliance with the apartheid regime in Pretoria. In December 1975, when Congress reacted by cutting off the CIA operation, that only ratified what was seen as the inevitable result—defeat—in the eyes of both Washington policy makers and the rest of the world.

In a longer perspective, neither the Iran nor the Guatemala operations can fairly be given too much credit—or too much blame—for what happened afterward in Iran and Guatemala. On one hand, TPAJAX restored the shah of Iran to his throne, where he remained for nearly a quarter century, a pro-Western bastion in a turbulent region. Twenty-five years of stability is no mean feat in international affairs. On the other hand, American covert action identified the shah's Iran more closely with the United States than was good for either of them.

In any case, however, the aspects of U.S. policy that loomed so large in the shah's downfall in 1979 were overt, not covert. They were his image as an American client, the waste and corruption associated with his massive U.S. arms purchases, and his own dependence on the United States. These factors owed much more to American policy during the 1970s than to the event of 1953.

A similar conclusion also applies to Guatemala in 1953. If, in retrospect, the "success" of PBSUCCESS also looks more ambiguous than it seemed at the time, most of the blame or credit lies with American foreign policy, not with covert action. PBSUCCESS did not make it inevitable that Washington would then forget about Guatemala; it only made it possible. David Phillips, a CIA officer who worked on PBSUCCESS, the Bay of Pigs, and Chile, laments that "Castillo Armas was a bad president, tolerating corruption throughout his government and kowtowing to the United Fruit Company more than his own people." But he argues that the United States "could have prevented this with the vigorous exercise of diplomatic pressure . . . to assure that he pursued social reform for the many rather than venal satisfaction for a few. Instead, Washington breathed a collective sigh of relief and turned to other international problems."[13]

Several covert operations of the 1950s remained secret for a long time: The CIA's assistance to Tibetans resisting the domination of their land by the People's Republic of China, regarded in intelligence lore as a successful holding action, is still a little discussed operation, especially because it is an embarrassment now that Sino-American relations have thawed. The effort to unseat President Sukarno of Indonesia, who had earned Washington's opposition for his espousal of nonalignment, ranged from covert political action to a paramilitary operation; it is not much better known than the Tibetan operation.[14]

Even in the 1960s, several brief and limited interventions—small in terms of numbers of people involved, though not in terms of purpose—remained secret for some time. So-called Track II—a secret effort to touch off a military coup in 1970 to prevent Allende from being seated as Chile's president, an operation run

without the knowledge of the State or Defense Departments—was not revealed for five years after it happened. And the sad plots in the early 1960s to assassinate Fidel Castro stayed buried for over ten years.[15]

CHANGING TARGETS, CHANGING TIMES

Yet times changed. Major covert actions became likely to become public knowledge—sooner rather than later, perhaps even before the operation was over. In 1986, the arms sales to Iran became public even though the leak did not initially come from Washington but from an article published in Beirut in Arabic. Americans became more skeptical of their government, of its information, and its capacity, a skepticism that is a legacy of the long history beginning with the label "Watergate." By 1986, when Ronald Reagan, the most popular president in generations, first denied that his administration had traded arms sales to Iran for the release of American hostages in Lebanon, most Americans did not believe him.

This skepticism has been reinforced by the prominence of investigative journalism; every cub reporter aspires to be Woodward or Bernstein of Watergate fame. The media now contain more people asking hard questions, even of secret operations, and probing for leaks; and there are fewer who are prepared to take the government at its word. If reporters are more likely to seek information on "secret" operations, so are they more likely to find it. Leaking, always present, has become routine in Washington; it has become almost acceptable. Officials sometimes leak information merely for the gratification of being pandered to by journalists more famous than they. More often, they leak to rally opposition to or (more rarely) support for a given policy. Administration after administration, regardless of its political persuasion, declares war on leakers. Those wars always fail. They fail for a simple reason: the ship of state is like no other, for it leaks from the top.

Officials at the top of government are precisely those who know of covert actions and thus are most likely to take their opposition to particular programs into the open. This is true of the executive branch, and all the more so of Congress, where this tendency is reinforced by institutional pride and often by partisan politics. On the whole the intelligence committees of the House and Senate have kept secrets at least as well as the executive branch. Yet their role in overseeing covert action means that those who might oppose a particular project are more likely to know of it. The process creates a set of frustrated opponents who will, on occasion, go public with their frustration.

Not every exposé, however, has created a controversy. Even now, not every covert action is controversial. Of the forty or so covert actions under way in the mid-1980s, at least half had been the subject of some press account.[16] Yet only several were controversial enough that the original leaks developed into continuing stories. Most of the rest were open secrets, more unacknowledged than

unknown; most members of Congress thought they made sense, as did most Americans who knew or thought about them—and, no doubt, most of the journalists who reported them.

Before September 11, 2001, the biggest open secret, or overt covert operation, was U.S. aid to those in Afghanistan resisting Soviet occupation of their country. Former CIA Director William Colby characterized the reaction to revelations of American assistance to the resistance in Afghanistan: "Afghanistan was a two-column headline in *The Washington Post* for one day, then almost nothing."[17] Americans in and out of Congress broadly supported the cause of the rebels, or *mujahedeen* (often called freedom fighters at the time, which became a cruel irony on 9/11), and the aid was a way to increase the cost of the Soviet occupation. American assistance reportedly begun in a small way in the last year of the Carter administration escalated sharply to reach as much as a half billion dollars a year by the late 1980s.[18]

The secret was an open one; the American role was not so much covert as unacknowledged, by tacit agreement. The reason for circumspection was the delicate position of the Pakistan government, the conduit for the American supplies to the rebels. Pakistan was prepared to support the rebels but was unwilling to be too visible in doing so lest it antagonize its powerful neighbor, the Soviet Union. In those circumstances, resorting to the CIA, rather than the American military, was more a matter of being discreet than of keeping the whole affair secret.

Certainly there will be cycles in American attitudes toward international threats, as there have been before. In the early 1980s most Americans evidently shared their president's concern with the Soviet threat, and their congressional representatives went along with huge increases in defense spending—and in covert action. Ronald Reagan was able to rebuild considerable authority and discretion in the American presidency, the Iran-*contra* debacle notwithstanding. After September 11, 2001, George W. Bush had at least as much of both support and authority. Most Americans enthusiastically supported the war in Afghanistan, and they were prepared, initially at least, to support the war in Iraq as a front in a longer fight against terrorism.

Still, if the changes in American domestic politics since the mid-1970s have made it more difficult for the United States to achieve its purposes secretly, other changes make it harder now than in the 1950s for the United States to intervene successfully at all, covertly or openly. Despite the controversy and mystique that surrounded covert action (and to some extent still do), history suggests that there is no magic to it. It means providing foreigners secretly with money, weapons, or training as tokens of American support.

With the passage of time, however, a little money here, a few weapons there became less likely to achieve grand foreign policy purposes. Castro was a target of a different order than Arbenz. To think in 1975 that a few million dollars might alter the fate of Angola was a faint hope at best, and an illusion at worst, especially given that the CIA recognized that the Soviet Union and other external actors might counter American support with more assistance of their own. Even

the CIA officials who planned the Bay of Pigs covert action knew that to delay the invasion until Cuba had received deliveries of advanced Soviet fighter planes would be to condemn the plan to certain failure.

Also, notice the contrast between two Central American cases three decades apart—Guatemala and Nicaragua. Castillo Armas's liberators numbered no more than several hundred. Their "invasion" was more conjured than real. Yet they had control of the air, in large part because Arbenz, unsure of the loyalty of his air force, was unwilling to risk putting his own pilots in the air. *Sulphates*—Spanish for "laxatives," the name Guatemalans gave to the invaders' bombs—plus rumors exaggerating the size of the invasion were enough to induce Arbenz to capitulate. In the case of Nicaragua, the contras numbered about 10,000 by the mid-1980s, yet not even the most ardent advocates of U.S. assistance to them argued that they were about to induce the Sandinistas to say uncle, much less that they posed a threat sufficient to overthrow the regime by sheer force of arms.

The makers of revolutions learned their own lessons from history, including the history of American covert action. They were determined not to repeat the mistakes of Arbenz and Mossadeq. They sought to assure themselves the loyalty of the army or to build revolutionary cadres of their own. Before the fall of communism, they also learned that if the United States threatened them, there were other sources of support to which they could turn. And, unlike Arbenz or Mossadeq, they turned to those sources sooner rather than later. Moreover, they learned that the United States could be very useful as an enemy. Arbenz, Mossadeq, and even Allende sought Washington's approval, or at least its acquiescence. By contrast, if the United States was of use to Castro, the Sandinistas, and the Ayatollah Ruhollah Khomeini, it was primarily as a foreign demon against which their revolutions could rally—even though the Sandinistas were prepared to accept American aid as long as it was forthcoming, and the revolutionary Iranians were not above seeking American spare parts for their military. In 1979 Iranians took Americans hostage and released them only when they ceased to be useful counters in the bargaining within the revolution. Suffice it to say that no one learned the value of America-as-enemy better than Osama bin Laden.

VALUES AND INSTRUMENTS

In all likelihood, the record shows, covert operations will become known, and America will be judged for having undertaken them. Thus, the practical lessons lead into moral issues. These issues are muted now by the fearsomeness of the terrorist threat. They are hardly unique to covert intervention, though they are powerfully present there, and they risked—and may still risk—being obscured in policy making by the presumption that covert actions will remain secret. Overt interventions, such as the American invasion of Grenada in 1983 or Panama in 1989, or military attacks, such as the bombing of Libya in 1986 or Sudan and Afghanistan in 1998, raise similar moral and instrumental concerns.

These concerns are not absolute; they must be considered against the gravity of the threat and the adequacy of other available responses.

In December 1976, when I was in Washington working with several old friends who were making arrangements for the transition between the Ford National Security Council (NSC) and the Carter NSC, we had decided to retain the basic structure of the Ford operation, with its network of sub-Cabinet committees for particular purposes. Yet of course, as a new administration, it was necessary to change the names of those committees, and so we joked about naming options. The 40 Committee, the Ford administration's group for discussing covert action, would become the "If They Can Do It, So Can We" Committee.

Yet, "if they can do it, so can we" did not seem, even then, to be an unacceptable rationale on either moral or instrumental grounds. What the Soviet Union or other nations did could not settle the issue, nor can how terrorists act. We consider ourselves different from them and imagine that the difference is not only basic to what we are as a people but also a source of American influence in the world, part of this country's moral armor.

We also believe that the example of democracy is powerful, one toward which peoples all over the world will gravitate if given the chance. Believing that, we must also believe that the example is a powerful part of our external behavior, not just of our internal arrangements. If people will choose democracy when given the chance, then democracy is demeaned, perhaps doomed to fail, if it is imposed from the outside. There is something incongruous about helping overthrow governments—especially ones that come to power through elections that we would define as tolerably fair (as in Chile in 1970)—in the name of democracy.

In this view, some of the successes of covert action seem, on the one hand, ambiguous or transient in retrospect, accomplished at significant cost to what we hold dear as a people and to America's image in the world. On the other hand, the world is a nasty, complicated place. The fight against terror has driven home that lesson. In that regard Americans' historical ambivalence between the high moral view and the feeling that international politics is a dirty business is understandable.

Terrorism aside, nations affect each other's politics in so many ways that any too-tidy definition of *intervention* is suspect. In all the examples cited, covert action formed only part of American policy. The United States decided whether to grant economic aid to Cuba, Chile, or Angola, and whether to release Iranian assets held in the United States. Most of these decisions were based on explicitly political criteria. Even if similar decisions toward other countries are not so clearly political, the decisions in any case have political effects on the country in question; foreign political leaders have no doubt of that fact.

The same is true of actions by private American actors. U.S.-based businesses either invest or do not invest in a country, and that decision too has not just an economic but also a political effect. That is the case even if the decision is not political in any narrow sense of the term. Most of the businesses or banks that chose not to invest in Chile under Allende probably did not make that choice for

any specific political reason, despite Washington's pressure. Rather, their decision was a business one, based on the climate in Chile. They saw that judgment as an economic one, though political instability surely was a factor in it.

In this context, if a unilateral self-denying ordinance against all intervention—open or covert—seemed too restrictive when the Soviet threat existed, it surely does now in an era of terrorism. Some threats to American national security require responses. Some American friends deserve support. What is imperative to keep in mind is the long-term costs of intervention for a government that is not notable for attending to long-term considerations.

Given that "covert" action is not likely to remain secret, why not act openly? In the case of aid to the FNLA and UNITA in Angola, covert rather than overt aid spared the first identification with the United States for only a few months; as for aid to the contras in Nicaragua, the "covert" form made not one whit of difference. The operation quickly became known, and the same was true of aid to the *mujahedeen* in Afghanistan. Nor is it obvious that in most of these cases that the recipients of American largesse minded the source of the money being known. There is also the risk that covertness creates a self-fulfilling prophecy: If the United States only aids its friends secretly, then any link to the United States may seem sinister, portending much more than is actually the case.

The scope for doing openly what might earlier have been done covertly has increased dramatically since the 1970s. Sovereignty has become less absolute, and international law has come to recognize people, not just nation-states. In that sense, international law has moved in a very "American" direction, even if Americans do not always like the results, as with the creation of the International Criminal Court. But international practice (if not law) has come to recognize that some behavior by national leaders justifies external intervention, even with force of arms.

American radio stations broadcasting into Eastern Europe and the Soviet Union from Munich, Radio Free Europe, and Radio Liberty, were private organizations in form; advertisements exhorted Americans to contribute to them. In fact, they were created and financed covertly by the CIA as propaganda vehicles. When that support was disclosed in 1967, the radio stations nevertheless continued to operate; they became supervised by a board and supported openly by appropriations from Congress.

In the 1980s, the Reagan administration was moved to create the National Endowment for Democracy (NED), on the model of the (then West) German party foundations, like the Konrad Adenauer Stiftung. They are instruments of the major parties but are supported openly by government money. They have openly assisted kindred parties and labor movements around the world. The NED, whose core budget reached $40 million in 2003, channels money to institutes of the two American political parties plus an AFL-CIO group and a business group, which then make grants in support of democratic institutions in a number of countries around the world.[19]

So far, the record of the endowment is mixed but hopeful. Its grants, and those of its four constituent institutes, began by being cautious and close to government policy. It remains an open question whether, given American politics, public funding is compatible with creative (and thus controversial) acts by private groups. The original NED budget was only an eighth of that of the German party foundations. Over the years, Congress has put a variety of restrictions on the endowment—for instance, in 1985 Congress halved the endowment budget and denied any funding to the Republican and Democratic institutes, although that prohibition was relaxed the next year. It may still be easier for the CIA to get money from Congress secretly than for another institution to get it openly—even if the purposes of the two are broadly similar. Funding for the CIA remains wrapped in the cloak of national security, so members of Congress may be prepared to fund particular activities but prefer not to be seen to vote for them openly.

Still, the endowment organizations have become more venturesome as the international and domestic climate has changed. More important, the endowment now works with scores of kindred organizations, both from other governments and from the private sector. To illustrate the change, in the mid-1980s, the NED provided more than $400,000 over two years to the American Friends of Afghanistan to develop educational and cultural facilities inside those portions of the country controlled by the resistance groups—activity that might in other times have been called the civic action component of a paramilitary operation.

By contrast, before Slobodan Milosevic fell from power in 2000, the endowment and other U.S. government sources openly funded opposition parties and groups to the tune of some $25 million.[20] Indeed, the whole operation was almost a carbon copy, done overtly, of what the United States had done earlier covertly in Chile, for instance. In the instance of Serbia, the main difference other than overtness was that U.S. government agencies had lots of company from other countries and private nongovernmental organizations (NGOs). In other respects, the post mortem could have been written by a CIA operative about Chile. For instance: "Foreign assistance should focus not only on political parties but should continue to support a broad range of nongovernmental organizations, labor unions, think tanks, and media."

Acting openly, however, is not always easy or a complete substitute for covert action. It requires an explicitness about influencing the politics of a foreign country that is uncomfortable for Americans and hence likely to be controversial. Moreover, governments that feel threatened by that open assistance can act to prevent it more easily than if it were covert. Yet even that ability is diminishing; national borders are more porous. Milosevic's Serbia did try to limit the assistance to opposition organizations. It had some success keeping foreign advisors out but much less success stopping money flows, and thus ended, somewhat paradoxically, with the worst of outcomes from its perspective: the antigovernment effort was well funded but harder to tar with the epithet "foreign influence" than it would have been had scores of foreign advisors been present. To quote the

post mortem again: "While foreign assistance helped to build and sustain the broad anti-Milosevic coalition, indigenous organizations and action were mainly responsible for driving events."

A bias toward openness has it limitations, but surely it is the right long-term direction for American policy. Openness would reflect the reality that, as the century ends, national boundaries are more and more permeable. Given this reality, moreover, those groups the United States would like to support may not be so chary of accepting help, even—perhaps especially—if it is open. The United States would say to them: "We are prepared to support you but only openly. We think that is better for you. In any case, we know it is better for us."

CHOOSING THE COVERT OPTION: LESSONS FROM HISTORY

The history of covert action before September 11, 2001, suggests that in deciding whether to choose the covert option, prudent policy makers should ask themselves a careful series of "what if" questions. That injunction applies to all policies, foreign and domestic. But it applies with special force to covert action because of the presumption of secrecy.

The most obvious "what if" is "what happens if—or more likely, *when*—it becomes public? What if it becomes public in midstream?" This is the *New York Times* test. Large covert actions will not remain secret, a reminder that is easy to state but hard to embody in the making of policy when the pressures go in the direction of wishful thinking. Witness the reflections on the Bay of Pigs invasion by Richard Bissell, then head of the CIA's clandestine service: "The argument was [not] made that this is now a very public business, and we'd better treat it as such, and either cancel it if we can't stand the publicity, or else do some of the things that will increase the chances of success if we are going to go forward with it."[21]

If the Iran operation of 1985–86 had remained secret for several years after all the U.S. hostages in Lebanon had been released, that success might have outweighed the costs of being seen to have traded arms for hostages when the operations became public. Perhaps. We cannot know for certain. It did not, however, take a sophisticated analysis to show that a covert policy targeted on some Iranians was vulnerable to being publicized by opposing Iranian factions if and when it suited their political purposes. And it was equally likely that when the cover was blown, trading arms for hostages with a nation the United States had denounced as terrorist would be deemed unacceptable—by America's allies, much of the rest of the world, and most important, the American people.

Of course, whether a particular covert operation can bear the test of disclosure is apparent in retrospect but often far from obvious before the fact. Prudence suggests that presidents pay careful attention to such warning signals as the review process throws up—the views of Cabinet officers, people in the White

House who attend to the president's interests, and congressional overseers who are surrogates for public reaction.

One warning signal, however, is evident in advance: Does the intervention contradict overt American policy? If it does, as with arms sales to Iran, it is especially improbable that the operation will withstand the test of disclosure. The arms sales were exactly the opposite of the administration's public policies, which had twisted the arms of America's allies not to sell arms to Iran, had sought an end to the Iran-Iraq war with neither a victor nor a vanquished, and had pledged not to bargain with terrorists over hostages, much less to sell arms to them.

A second "what if" is "what if the first intervention does not succeed? What then?" If covert action is to remain secret, most of the time it will have to be small. Small operations have often begun with grand purposes, objectives incommensurate with the instrument. When the goals could not be achieved, leaders were tempted to take the next step and the next. This happened in the Bay of Pigs invasion, Angola, and Iran in the mid-1980s. Sometimes a limited objective can be achieved, but its achievement makes it appealing to hope for more—witness Angola and perhaps Nicaragua, where the United States did seem to achieve its initial aim of cutting weapons supplies from Nicaragua to the antigovernment rebels in El Salvador. Answering this "what if" suggests, at a minimum, careful attention to the CIA's covert operators themselves, for signs of skepticism about whether operations as initially conceived can achieve their purposes. Such signs were present between the lines of Track II in Chile, Angola, and Nicaragua. Some risks are worth running, but few are worth running in ignorance.

A third set of "what if" questions is "what signal will be received, by whom and with what result?" These judgments are also easier with the benefit of hindsight, for they involve calculations of threat and of American interests. Intelligence assessments by the CIA or the State Department provide one set of indicators. In 1985–86, for example, American intelligence on Iran was weak, but what there was offered precious little ground for believing there were moderates who might be detached from their revolutionary colleagues. Later U.S. intelligence cast doubt on the imminence of a Soviet threat to Iran, one of the original premises of the operation. These were cautions that the intended signals might go awry.

The nature of those who are to receive secret American assistance can provide another warning signal. Because their relationship to the United States is meant to be clandestine, the CIA is often in a weak position to compel them to act to suit American purposes, yet the United States inevitably will become associated with their actions, like it or not, if and when the fact of support becomes known. Aid to the contras was dogged by their origins in Somoza's hated National Guard and by charges of human rights violations. Similarly, support for resistance forces in Afghanistan could have been justified as a way to put strategic pressure on Soviet occupation of that country; but given the character of the

resistance forces, it was hardly a way to bring democracy to Afghanistan—far from it.

The regional context, in particular the attitude of American friends in the region, is another source of guidance. In the instance of Afghanistan, American assistance to the resistance was supported, though with varying degrees of publicity, by nations ranging from Pakistan and Egypt to Saudi Arabia and China. In Central America this indicator was more ambiguous, for most of the nations of the region publicly expressed qualms about the aid to the contras while privately hoping the Sandinistas could be made to go away.

The second round of covert action in Angola raised these questions of signals given versus those intended, questions for which the 1975 episode provided guidance. In early 1986, the CIA was authorized to provide $15 million in weaponry to Jonas Savimbi's UNITA. For the Reagan administration, the intended signal was anticommunism. For the administration, there was nothing incompatible about supporting anticommunism in Angola and antiapartheid in South Africa. Alas, the reality of southern Africa frustrated that conception in the heads of Washington policy makers. Whatever his attractions, Savimbi had one flaw, a fatal one: he was almost completely dependent on South Africa, his army almost a unit of South Africa's. To support him was to signal to Africans that the United States was throwing its lot in with South Africa, in 1986 just as in 1975.

These rules of thumb amount to establishing a presumption against covert action. The guidance is mostly negative, a series of cautions. It is unwelcome to officials who are looking for something to do rather than something to avoid—a trait that runs deep in the American character and is reinforced by the circumstances in which covert action becomes an option. Yet given how both America and the world have changed over the postwar period, the circumstances in which major covert action makes sense as policy are sharply limited.

Guidelines akin to these were articulated in the 1970s by Cyrus Vance, later Secretary of State. For Vance, the criterion for covert action in the National Security Act of 1974—"affecting the national security"—was too loose. Instead, he recommended covert intervention only as an exceptional measure, when it was "absolutely essential to the national security" and when no other means would do.[22] Decisions would still be matters of judgment under this more restrictive guide, but no one has improved on the Vance standard.

COVERT ACTION SINCE SEPTEMBER 11, 2001

How has covert action changed since 9/11? And how do those changes relate to the lessons from earlier operations? Most strikingly, 9/11 underscored all too dramatically another theme from my review of earlier covert actions—the problem of control. The very fact that the interventions are meant to be covert gives rise to special problems of control. The link between U.S. intentions and the

actions of those foreigners is tenuous at best. They are acting; the United States is only helping. Their purposes may not be ours. They have every incentive to hear from their CIA liaisons what they want to hear or construe it to their own purposes. In the details of earlier operations, that meant that covertly supported groups sometimes engaged in a little unsanctioned drug dealing or killing along the way or tried to overturn regimes when the United States only thought it was keeping opposition forces alive.

In supporting the anti-Soviet *mujahedeen* in Afghanistan, however, the problem of control was strategic. To minimize the American role, the CIA provided mostly money. Most of the contact in Afghanistan with the *mujahedeen* was done by Pakistan's Inter-Services Intelligence (ISI). For its own and Pakistani reasons, ISI gave preference to the radical Islamists among the *mujahedeen*, and in doing so, sowed the seeds for the takeover of Afghanistan by the Taliban and the formation of Al Qaeda as a unified fighting force. "Their" purposes were manifestly not "ours." The two sets of purposes converged only so long as both wanted to expel the Soviet Union from Afghanistan.

In that sense, the problem of control merges with the more general problem of longer term, unintended side effects, one that afflicts not only foreign policy but all of human action. In this case, however, as in most others, it seems unlikely that any amount of asking "what if" could have changed the decisions in the 1970s and 1980s. The "what if" was simply too iffy. The Soviet Union was there in Afghanistan. Getting it out, somehow, was more than U.S. policy makers at the time could hope for. No story about the trail from ISI support to the Taliban to Al Qaeda to collapsing towers could have been made vivid enough to change the decision. The most that might have been accomplished would have echoed David Phillips's comment about Guatemala a half century earlier: support for the *mujahedeen* didn't have to entail that the United States would forget about Afghanistan after the Soviet Union departed.

One big part of the change in covert action happened before 9/11, as Serbia illustrated. Given the end of the Cold War and the changing currents in international law and attitudes, the CIA seems all but out of the business of Chile-style political actions to sustain opposition forces or overturn regimes. In 2006, the Bush administration proposed major funding in support of Iranian opposition groups, but it did so openly, through the State Department. There may arise cases in which covert funding seems imperative—it is hard to imagine supporting North Korean opposition elements at all, and surely impossible openly—but they should be rare. In promoting democracy, or even regime change, the world has transformed enough to allow the bias toward openness to prevail, along with the bias toward company.

To that extent, covert action has become, post-9/11, primarily paramilitary, with the CIA operating either independently or, more often, with military special operators. Surely, the CIA's performance as the first Americans in Afghanistan was impressive.[23] Its operations were secret only in their tactical details, and thus

met the *New York Times* test. The national investigation of 9/11 lauded that CIA role and the Afghanistan precedent of joint CIA-military teams. It recommended, though that the CIA cede responsibility for directing and executing operations to the military, with agency officers and capabilities integrated into military-directed teams, giving both the CIA and the Special Forces the opportunity to do what each does best.[24] The December 2004 intelligence reform bill was silent on this issue, and the CIA and the military decided that both would remain in the paramilitary operations business.

Which agency is responsible for conducting paramilitary operations has been at issue well before 9/11, driven by Vietnam and other episodes. The arguments for giving the military control have been, historically, the ones the 9/11 Commission cited: the requisite capabilities are military, the task has not been a continuous priority for the CIA, and it makes no sense for the nation to build two parallel capacities. Operations by the military would give those carrying them out the status of combatants under international law, at least if they were visibly soldiers. On the other side is the concern that the military was never very agile or discreet, let alone covert. That concern may have diminished, but not disappeared, as the special forces have developed a wide variety of units and types of operations.

Whatever else is occurring, the special forces and the CIA are being thrust together, and the CIA is being pushed into counterterrorism operations, both with the military and independently. Both kinds of operations raise thorny questions of authorization and accountability. In 2002, CIA operatives killed five suspected Al Qaeda operatives in Yemen with a Predator missile fired from an unmanned aerial vehicle (UAV). One of the five was a U.S. citizen.[25] The CIA conducted a similar attack in 2006 along the border between Pakistan and Afghanistan.

CIA covert operations require a presidential finding, one transferred in secret to the relevant committees of Congress.[26] Existing findings apparently provided authorization for the CIA to conduct both Predator attacks. By contrast, a similar operation conducted by military special forces could be set in motion simply by the chain of command from the president as commander-in-chief. Unfortunately, the difference may be less than meets the eye, however, if findings have become so broad in the war on terror as to cover almost any CIA operation. If so, however, the problem lies with the breadth of the findings. If they are so broad as to cover almost anything, then the finding process has become a sham.

COVERT ACTION AND OPEN DEMOCRACY

The United States will remain in the business of covert action. It will continue to confront the paradox of secret operations in a democracy, even if those operations are mostly paramilitary and counterterrorist in character. Unfortunately, the process of congressional oversight of intelligence, including covert

action, so carefully crafted in the 1970s, is now regarded as something of a joke in Washington. Terrorism is frightening enough to the body politic to justify almost any action in response—though the controversy in 2006 over eavesdropping on Americans by the National Security Agency in the wake of the terrorist attacks of 9/11 emphasizes the "almost." The House and Senate oversight committees have not escaped the bitter partisanship that has come to afflict Congress as a whole, and for a variety of reasons, the stature of the committee members has declined, though with several sparkling exceptions.

The 9/11 Commission suggested that if a single national intelligence director is to oversee the entire intelligence community—and preside over funding for all of it—Congress also should concentrate its oversight. Accordingly, the commission called on Congress to renew its commitments from the 1970s, having either a single joint committee to oversee intelligence (on the model of the old Atomic Energy Committee) or single committees in each house. Like the House Homeland Security Committee after them, the intelligence committees were never given the monopoly that was intended at their creation, and through the years even more committees have become involved.

The commission also sought to revamp ideas from the 1970s agreements in several other ways. To represent other committees with interests in the field, the new oversight committee or committees would revert to the practice of having a member who also serves on each of the following committees or subcommittees: Armed Services, Judiciary, Foreign Affairs, and Defense Appropriations. To promote continuity and expertise, oversight committee members should serve indefinitely on the new intelligence committees. The new committees should be smaller—perhaps seven or nine members in each chamber of Congress—so that each member feels a greater sense of responsibility and accountability for the quality of the committee's work.

Here, too, the arguments are of long standing, running back to the congressional investigations of the 1970s. However, changing times reshuffle the arguments. Surely the idea of having real focal points is the right one. The objective was identical in the 1970s, but it was never fully achieved and has eroded since then as more committees have gotten into the act. In those days, the model favored by the 9/11 Commission, a single committee for both houses on the Atomic Energy Committee model, was not in favor, for it was regarded as having become the captive of the agency it oversaw. That fear that permanent committee members might become too cozy with the agencies they oversaw also led Congress in the 1970s to give the intelligence committees rotating memberships.

Now, however, those memories are distant and the need for focal points more intense. To try to achieve those points, the commission also favored the 1970s practice of appointing members from other committees with stakes in intelligence to the oversight committees. So, too, by the lights of 2004, when the commission reported, the need for experience on the oversight committees outweighed concerns over cooption, and so the commission favored open-ended assignments to

the committee or committees, not rotating ones. But these are details. The real challenge for Congress is not to lag too far behind the executive branch in its own reshaping for the intelligence challenges of the twenty-first century.

The Iran-*contra* affair two decades earlier showed how difficult it can be to manage the paradox of secret operations in an open society. When the president finally signed the finding in January 1986 for the Iran arms sales operation, that finding was explicit: do not tell Congress. The congressional overseers did not find out about the Iran operation until autumn—hardly the law's requirement of "fully and currently informed" by anyone's definition. Later on the president himself apparently was not told, when the Iran and *contra* operations crossed with proceeds from the arms sales to Iran used to fund the contras without congressional appropriation.

In another sense, however, the system worked. In deciding to sell arms to Iran, the president pursued a line of policy opposed by both his Secretaries of State and Defense, about which he was afraid to inform the congressional intelligence committees and which was liable to be revealed by Iranian factions when it suited them. It is hard to imagine any system providing more warning signals. When most of the government's senior foreign policy officials are opposed, it is likely that the policy is wrong. The president thus proceeded at his own peril.

With regard to the diversion of money for the contras, the lesson is a caution for presidents and those who advise them: do not run covert operations from the White House. Before the 1970s it would have been unthinkable for an administration to do so; then the reason was that presidents wanted to stay at arm's length from such things, even if they could not plausibly deny them in a pinch. Now, though, if covert actions are to be undertaken, they should be done by the agency of government constructed to do them—the CIA. It has both the expertise and the accountability.

Moreover, the history of covert action suggests that if the president's closest advisors become the operators, the president loses them as sources of detached judgment on the operations. The president's own circle become advocates, as Allen Dulles did in the Bay of Pigs invasion, not protectors of the president's stakes (even if he does not quite realize his need for protection). So it was with Reagan's National Security Advisors, Robert McFarlane and John Poindexter; once committed, they had reason to overlook the warning signals thrown up by the process. Excluding the designated congressional overseers also excluded one more "political scrub," one more source of advice about what the American people would find acceptable. And the chances increased that someone like Lt. Col. Oliver North would misguidedly interpret the president's interest after his own fashion.

William Miller, the staff director of the first Senate Intelligence Committee, reflected on the Iran-*contra* affair: "If clear lines hadn't been drawn a decade ago, there would have been no hue and cry now."[27] Now is the time to remember again those lines and draw them again, all the more so as the boundary between covert action and military special operations blurs.

NOTES

1. For an assessment by a fellow staffer, see Loch K. Johnson, "Congressional Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee," *Public Administration Review* 64 (January 2004), pp. 3–14.

2. See *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate*, 94th Congress, 2nd sess. (1976). For links to these reports, as well as to a rich range of other documents, both historical and contemporary, see www.icdc.com/~paulwolf/cointelpro/cointel.htm.

3. The "40" merely referred to the directive that had created the committee. At other times, in modest attempts at discretion, the committees had been named for the room in which they met.

4. Gregory F. Treverton, *Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, 1987). This chapter draws on an article produced from the book, Gregory F. Treverton, "Covert Action and Open Society," *Foreign Affairs* 65, no. 5 (Summer 1987).

5. For an authoritative account of the affair, see *Report of the President's Special Review Board* (the Tower Commission) (Washington, DC: Government Printing Office, 1987). The *Final Report of the Independent Counsel for Iran/Contra Matters* (1993), is available at http://www.fas.org/irp/offdocs/walsh.

6. Reprinted in William M. Leary, ed., *The Central Intelligence Agency: History and Documents* (Tuscaloosa: University of Alabama Press, 1984), pp. 131–33.

7. Cited in Kermit Roosevelt, *Countercoup: The Struggle for the Control of Iran* (New York: McGraw-Hill, 1979), p. 199. Because Roosevelt's account is not independently documented, his recollections should be taken as evocative, not gospel truth.

8. The most authoritative account of the Guatemala intervention is Richard H. Immerman, *The CIA in Guatemala: The Foreign Policy of Intervention* (Austin: University of Texas Press, 1982), though additional details have been declassified more recently.

9. Quoted in Theodore C. Sorensen, *Kennedy* (New York: Harper & Row, 1965), p. 309.

10. The best account of covert action during this period is *Covert Action in Chile*, staff report to the Senate Select Committee . . . on Intelligence Activities, 94th Congress, 1st sess. (December 1975).

11. See, for example, Conor Cruise O'Brien, "How Hot Was Chile?" *The New Republic*, August 26, 1985, p. 37.

12. Author's press briefing on behalf of the Church Committee, Washington, DC, December 4, 1975.

13. David Atlee Phillips, *The Night Watch* (New York: Atheneum, 1977), p. 53.

14. For accounts of both, see chapters 8 and 9 of John Prados, *Presidents' Secret Wars: CIA and Pentagon Covert Operations Since World War II* (New York: Morrow, 1986).

15. Both Track II and the anti-Castro plots are detailed in *Alleged Assassination Plots Involving Foreign Leaders*, an interim report of the Senate Select Committee . . . on Intelligence Activities, 94th Congress, 1st see. (November 20, 1975).

16. This number is rough, based on my interviews at the time and on press accounts. In any case, the precise number does not mean very much because operations vary widely in cost, not to mention risk and degree of controversy.

17. Interview with author, Washington, DC (January 9, 1986).

18. See Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001* (New York: Penguin Press, 2004).

19. The NED's website contains a careful history of the idea and organization, one that is self-aware of the constraints on NED's operations. See http://www.ned.org/about/nedhistory.html.

20. For this figure, the following quotes, and a nice summary of the Serbian case, see United States Institute of Peace, *Whither the Bulldozer: Nonviolent Revolution and the Transition to Democracy in Serbia,* Special Report 72, 6 August 2001, available at http://www.usip.org/pubs/specialreports/sr72.html.

21. Interview, Columbia University Oral History Research Office (1967), p. 25.

22. Testimony before the Senate Select Committee . . . on Intelligence Activities (Dec. 5, 1975).

23. As usual in Washington, if success didn't have a thousand fathers, it surely did have a thousand chroniclers. Among many accounts of the CIA's role, see Gary C. Schroen, *First In: How the CIA Spearheaded the War on Terror in Afghanistan* (New York: Random House, 2005).

24. Formally, the National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (Washington, DC, 2004), available at http://www.9-11commission.gov (accessed August 2, 2004). The specific recommendations are summarized in the Executive Summary and spelled out in more detail in chapter 13, "How to Do It? A Different Way of Organizing the Government."

25. See Dana Priest, "U.S. Citizen Among Those Killed in Yemen Predator Missile Strike," *Washington Post*, November 8, 2002, available at http://www-tech.mit.edu/V122/N54/long4-54.54w.html; Walter Pincus, "U.S. Strike Kills Six in Al Qaeda: Missile Fired by Predator Drone; Key Figure in Yemen Among Dead," *Washington Post*, November 5, 2002, p. A01, available at http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A5126-2002Nov4&notFound=true (accessed April 25, 2005).

26. The term *finding* comes from the Hughes-Ryan Act of 1974, which required the president to "find" a particular operation necessary to U.S. national security. Turned into a noun, that became a finding delivered in secret to relevant committees of Congress.

27. Interview with author, Washington, DC (January 16, 1987).

2

COVERT ACTION

The "Quiet Option" in International Statecraft

KEVIN A. O'BRIEN

INTRODUCTION

SINCE THE DAWN OF THE NATION-STATE IN international relations, great powers have attempted to control and, if necessary, destroy other powers in a quest for world dominion and control. The nineteenth and twentieth centuries saw the evolution of these policies into refined, fully developed state actions throughout the world, dominated by a few powers alone. The mechanisms and methods used in this quest evolved over time, in most cases becoming more refined and successful—and generally involved three categories of activities: diplomacy, war, and "statecraft," the latter the activities of states when neither of the first two activities were viable options. Indeed, it would appear that these mechanisms of state power developed to their fullest in the post-1945 era, when the third option—statecraft and its primary instrument, covert action—became the mainstay of the Cold War.

Covert action is often been referred to as "the quiet option," both in terms of the intelligence activity and—more broadly—international relations. Used throughout human history, it became—much like the rest of the intelligence activity—a formalized, bureaucratized element of intelligence during the twentieth century. Reaching its height during the Cold War, during which it was used extensively by both East and West blocs in pursuit of both their geostrategic interests and their own rivalry, as a tool it has witnessed a few changes since the end of the Cold War.

Over the past three decades, particularly within the institutions of U.S. governance, covert action has been both far more broadly defined and constrained under legislative and executive statutes and norms; however, this has not meant an end to the use of covert action as a tool of state policy—far from it. Although

today covert action would appear to be less of a concern to those interested in the oversight and accountability of intelligence matters and activities, it has remained an often used tool of states around the world. Much like during the Cold War—and for decades, if not centuries, before it—covert action continues to be a tool used to support states' interests and rivalries around the world.

This chapter discusses the "uses and limits" (as Treverton refers to it) of covert action over history, outlining the different categories of covert action witnessed and the utility to which each was put. I provide examples as case studies of these uses and limits, and will consider the implications and impact of the use of each category of covert action outlined. I outline these uses in the different historical periods considered—war, peace, in the shadow world of the Cold War, finally considering "wither covert action today" as the post–Cold War interregnum came to a close in mid-2001 and the twenty-first century's first global war—the war on terrorism—began. My focus centers heavily on the United States (most particularly) and the Soviet Union during the Cold War—both because covert action was very much *the* tool of the Cold War's bipolar confrontation and because assessing quantifiable data on covert activities more recently is difficult (given their recent occurrence)—with other countries providing examples throughout.[1]

DELINEATING COVERT ACTION

In many ways, covert action (CA)—referred to by the Soviets as active measures—reached its height during the Cold War in terms of the extent of its uses, the bureaucracy that developed to support it, and the interest that was taken in it by the public. The scope of CA is very broad—Johnson calls it the "'third option' between diplomacy and open warfare"[2] placed firmly between these options; Godson defines it simply as "the attempt by a government to influence events in another state or territory without revealing its involvement."[3] Its covert nature allows states to use it when the first option—diplomacy—is insufficient to achieve an aim, but the second—warfare—is not an option. In British terms, covert action was always seen as "special political action," emphasizing its direct linkage to policy.[4] According to official American definitions—or, at least, delineations of covert activities—it constitutes both "such other functions and duties related to intelligence affecting the national security" and "activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the [government] is not apparent or acknowledged publicly" (according to the 1947 U.S. National Security Act and Executive Order 12333 signed by President Reagan in 1981).[5] This latter element—the fact that this option is chosen by governments when they do not want their presence or hand acknowledged or notable, granting "plausible deniability"—is central to appreciating all aspects of CA. Such catchall phrases have—in the U.S. case, legally speaking—allowed for the undertaking of significant covert activities by

the government in a manner that attempts to find the balance between the stagnancy of diplomacy and the risk of overt military force.

The key categories of CA are *propaganda* (also referred to as psychological operations), *political CA* (CPA), *economic CA*, and *paramilitary CA*.[6] Each will be explored in greater depth in this chapter.

Godson also provides a distinction between covert action and counterintelligence, where the latter is "targeted at adversary intelligence operatives and their political masters" compared to the former which targets "non-intelligence players"—this distinction is as true in the twenty-first century as it was during the Cold War.[7] Finally, covert action is linked to but not an element of the intelligence process: it can both contribute and react to intelligence. As Steiner warns recently, CA is "the most sensitive technique for implementing national security policy. . . . [CA] is all about making things happen, while intelligence consists of making the right decisions about what to make happen."[8]

COVERT ACTION THROUGHOUT HISTORY

Since the dawn of time, CA has been used as an element of societies both conducting intelligence activities against each other and wishing to undermine each other. Examples throughout history are manifold—a key example of covert action was the bribery of foreign officials and rulers as a means of persuasion. As Blackstock notes, throughout the eighteenth century, the major European powers used secret state funds extensively (and unsuccessfully) to bribe various foreign leaders to their cause—such as in Sweden in the 1740s, when England, France, Russia, and Denmark spent enormous sums on the bribery of political party leaders, with little result.[9]

During periods of war in the twentieth century, CA was used extensively. In World War I, the so-called Campaign in the Desert carried out by Lawrence of Arabia saw a key, covert sabotage and destruction raiding element deployed—using British officers and Arab (Bedouin) tribes to both distract the Ottoman Turks (whom, as allies of Imperial Germany in the War, the British were fighting in the Middle East) and press the British advantage in capturing and securing large territories in the Middle East against French and American interests. Such guerrilla warfare tactics that Lawrence developed became the touchstone for similar activities in the post-1945 decolonization wars and the example on which most Western covert paramilitary insurgency/counterinsurgency tactics were predicated.[10]

As World War I drew to a close and the Russian Revolution and subsequent civil war gathered momentum, the teeter-totter of the twentieth century's global conflict between the forces of worldwide communism and capitalism began to deploy CA as a key element of the struggle between them. Though such activities came into their prime during the Cold War period, during the interregnum of 1917 to 1939, CA was used widely by newly established Soviet Russia to both

counteract the activities abroad of anti-Bolshevik elements (especially in the United Kingdom and United States) and to begin the spread of world socialism through the Communist International as the first stages of worldwide socialist revolution. One of the best (and most successful) examples of this in history was the Monarchist Association of Central Russia, better known as "The Trust": targeting White Russian émigré groups in a massive deception operation aimed at penetrating these groups and flushing out remaining White Russian supporters and sympathizers back in Soviet Russia.[11]

In Ireland, following the 1916 Easter Rising, the newly formed Irish Republican Army under Michael Collins used covert tactics to harass, assassinate, and sabotage institutions and individuals of British power in Ireland during the Irish War of Independence (1919–21)—and later the opposing side in Irish civil war (1922–23)—so successfully that his activities became the template for covert urban and rural paramilitary operations for the rest of that century.[12]

During World War II, CA was used extensively in many forms—economic, political, paramilitary and (certainly) psychological—to support the overt war operations. Indeed, it could be said that the war began with a covert paramilitary operation that simultaneously had an extreme propaganda intention: the deployment of German soldiers, SS men dressed in Polish uniforms (in their own pseudo-operation), and dead concentration camp inmates at the German-Polish border to give the impression that Germany had been provoked into counterattacking Poland on September 1, 1939.

The May 1942 assassination in Prague of SS intelligence chief Reinhard Heydrich by Czech partisans working with the British Special Operations Executive (SOE) is a prime example of assassination as a form of covert paramilitary action. Indeed, the very establishment of the SOE, its sister organization the Political Warfare Executive, and the U.S. Office of Strategic Services (OSS) were all aimed at establishing the ability to conduct covert operations against Axis interests throughout the territories that they occupied during the war. Significant deception operations—such as the Double-Cross System used in the intelligence war between the British and Germans on the personal level and Operation FORTITUDE, the massive deception operation used to support the D-Day landings, on the grand strategic deception level—were played out as a component of both covert political action and psychological operations. Overall, the quantity and variety of covert actions deployed during World War II was massive.[13]

COVERT ACTION DURING THE COLD WAR

It was truly during the period since 1945—centered on the Cold War period—when covert action came into its prime as one of the key elements of statecraft. The Cold War could be appreciated as "a war carried on by means short of sustained, overt, military confrontation," implicitly conveying the understanding that the confrontation between the Western world (dominated by the United

States) and the communist bloc (dominated by the Soviet Union) was covert in nature—resorting more often than not to nonmilitary means in an attempt to undermine the authority of the opposing power while maintaining control and influence over their own sphere. This clash was not unforeseen: Lenin stated in 1921 that "the existence of the Soviet Republic side by side with the imperialist States is in the long run unthinkable . . . a series of the most terrible clashes between the Soviet Republic and the bourgeois States is unavoidable."[14]

In this sense, therefore, the origins of the use of covert action during the Cold War lay with the governments of both the United States and the Soviet Union and their interactions both between the years 1919 and 1939 and during World War II. The main concern of the United States (as well as significant Allied countries, such as the United Kingdom, Canada, and Australia) was the growth in communist influence within Western societies. This increased until, during the period following the early days of the Cold War, it was perceived as "the global challenge of Communism . . . to be confronted wherever and whenever it seemed to threaten our interests."[15] Ultimately, as Maurer has pointed out, whereas the United States—like most democratic countries (as well as leading regional powers such as South Africa or India)—tended to distinguish between overt and covert activities, "the Soviet Union [placed] a premium on influencing other countries' beliefs about both itself and the [United States], and that the Soviets [made] little distinction between overt and covert means [in so doing]"—an important distinction to keep in mind throughout this chapter.[16]

Covert action during the Cold War symbolized an ideological conquest for the soul of the world that was the basis of the rivalry between the Western and Soviet (East bloc communist) intelligence services. Within the period of 1945 to 1991, both powers developed their security and intelligence services as a mechanism by which this confrontation could be carried out; in the United States, the Central Intelligence Agency (CIA) was founded in 1947 for (originally) the purpose of intelligence collection and dissemination. In the Soviet Union, the KGB was reorganized out of the previous intelligence and security services following Stalin's death in 1953. Both services soon rapidly developed covert action arms that far outweighed their intelligence collection missions. In the case of the KGB, such activity had been the mainstay of the previous incarnations of Soviet security (Cheka, GPU, OGPU, NKVD, MGB, MVD), whereas the United States had only developed such an ability with the founding of the OSS during World War II—which was disbanded at the end of the war, two years before the founding of the CIA.

The Development of U.S. Covert Action

In any discussion of covert action—particularly within the Cold War context—the United States provides some of the best (and worst) examples. Covert action is an instrument of statecraft that the United States had long deployed (as with any other power) over the course of its development and expansion (at the

least, following the 1898 Spanish-American War). In the post-1945 period in its confrontation with the Soviet Union—both directly and, more frequently, indirectly—the United States used CA extensively and increasingly. Given the nature of the Cold War, CA became the tool for the United States to deploy to both further its interests and undermine its adversaries, particularly the Soviets, in pursuit of their own interests. Indeed, the establishment of the primary tool—the CIA—by which covert actions were developed and used changed the entire raison d'être of the agency as it was originally envisaged. Covert action developed largely due to the plausible deniability implicit in its definition, and the official delineation of CA ("such other functions and duties related to intelligence affecting the national security," as taken from the 1947 National Security Act) provided foreign policy makers the "allowance" to use the CIA to conduct clandestine operations as its primary mission, rather than the collection and dissemination of intelligence as the original formers of its mandate envisioned. This has been further institutionalized by the Executive Orders of successive presidents.[17]

This is not to say that using such means are peculiar to the post-1947 period in U.S. foreign policy. In reality, the use of such covert actions in U.S. foreign policy took flight at the end of the nineteenth century with the Spanish-American War but began their development much earlier. Although a complex subject unto itself, such capabilities and operations that were later inherent to American covert activities abroad were the direct descendants of the methods of intervention, control, and subversion that the United States deployed—particularly in Central and South America—as part of its Monroe-driven hemispheric hegemony during the second half of the nineteenth and first half of the twentieth centuries. These included the processes of direct and indirect interventions, the use of front or partner organizations (such as the United Fruit Company) in assisting with such control, and the deployment of covert economic and political activities to further those methods of control. By the 1950s, these same approaches had matured into fully developed covert action capabilities.

The Growth of U.S. Covert Action Capabilities

Despite the growth of its covert (and overt) intervention and control capabilities during the previous 100 years, by 1941 the United States—unlike the Soviet Union, the United Kingdom, and virtually every other major power in the world—still did not have an established intelligence service. The attack on Pearl Harbor caused the United States to seriously reexamine their intelligence abilities, as this came to symbolize the worst failure ever of intelligence facilities in modern times.[18] Realizing that it could never again suffer such a surprise attack and to avert it from happening again, the U.S. government determined that it would be necessary to establish a foreign intelligence service with the aim of information collection, covert action, and counterintelligence.

In July 1942, Roosevelt established the Office of Strategic Services (OSS) to coordinate and develop methods of subterfuge and covert warfare. At the end of World War II, Truman abolished the OSS as unnecessary in its current form, having been designed for war. But it was soon apparent that the need for strategic intelligence, which had been divided up under control of the various branches of the military and state departments, would be of increasing importance as tensions began to build with the Soviet Union. The framework for this was pronounced in Kennan's famous article, "The Sources of Soviet Conduct", in which he stated that "in these circumstances it is clear that the main element of any United States policy toward the Soviet Union must be that of a long-term, patient but firm and vigilant containment of Russian expansive tendencies . . . by the adroit and vigilant application of counter-force at a series of constantly shifting geographical and political points, corresponding to the shifts and maneuvers of Soviet policy."[19] The worldview that this professed was further outlined in Eisenhower's secret 1954 National Security Council (NSC) memorandum, which stated: "If the US is to survive, long-standing American concepts of 'fair play' must be reconsidered. We must develop effective espionage and counterespionage services. We must learn to subvert, sabotage and destroy our enemies by more clear, more sophisticated and more effective methods than those used against us."[20] This centered on the idea that the Soviets would need to be confronted throughout the world on an increasingly involved level; this led Truman to institutionalize, through the Department of Defense and the Central Intelligence Group (later Agency), the military and intelligence/covert bureaus as the key arms of conducting this covert foreign policy.

In 1946, Truman established the Central Intelligence Group (CIG), modeled on the OSS; on July 26, 1947, the National Security Act was passed by Congress, replacing the CIG with the CIA and establishing the NSC as the sole advisory committee reporting directly to the president on matters of national security. This was followed two years later by the Central Intelligence Agency Act, which further defined the CIA's mandate.[21] As one of the five directives granted it by the National Security Act, the CIA was authorized to "perform such other functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct."[22] The ambiguity found in this directive was included to "provide flexibility to the newly created CIA in order to meet unforeseen challenges."[23] In reality, it was perceived to grant the authority to undertake covert actions around the globe as often as it liked without the necessity of congressional approval, some of which came dangerously close to undeclared war operations against foreign governments.

U.S. Covert Action During the Cold War

Contemporary politics had a great deal to do with the origins of the policies related to covert action. In the case of the CIA, Europe during the late 1940s and

into the 1950s was the United States' prime concern. Reconstruction was being carried out in Western Europe, but communist influence was strong. Politically in Italy and France, the communists threatened to destabilize the postwar political and economic balance that the United States was attempting to establish throughout the Western world. In addition, communist unions and organizations posed serious threats to the economic and social welfare of rebuilding Europe. In support of this covert confrontation within the emerging Cold War, the Covert Action Staff (CAS) was established within the CIA and given the Kennan-esque task of rolling back communism, initially in Europe.[24] The CAS—residing initially in the Office of Special Operations, which gave way to first the Directorate for Plans and later the Directorate of Operations—was to serve as a complementary branch to the Office of Policy Coordination (OPC)—itself founded in May 1948 on Kennan's encouragement and intended to "undercut debilitating strikes by Communist trade unions and election advances by Communist parties."[25] These operational roles were laid out in not only the National Security Act of 1947 but also in directives like NSC 10/2 and NSC 5412/2.[26] NSC 10/2, passed on June 18, 1948, by Truman, stated that "the overt foreign activities of the US Government must be supplemented by covert operations," which initiated the CIA's program of propaganda and paramilitary action against the Soviet Union. These operations could involve activities "up to a level just short of armed conflict by recognized military forces."[27]

This policy can be clearly summarized in three points: create and exploit problems for international communism, discredit international communism and reduce the strength of its parties and organizations, and reduce international communist control over any areas of the world.[28] More directly, as Marchetti and Marks state, "in most countries . . . the United States policy [was] usually to maintain the *status quo*, so most [CIA] subsidies are designed to strengthen the political base of those in power."[29] But the status quo could prove difficult to maintain, as Kolko notes: "The credibility of American military power and the emergence of geopolitical analogies and linkages in the form of the domino theory soon subjected US behavior and policies in many areas to new influences that paralleled and sometimes outweighed the more traditional narrower assessments of the economic and political stakes involved in success of failure, action or inaction, in some nation or region." This in turn led to "A growing number of de facto and formal alliances with Developing World surrogates . . . raising for the first time the United States' increasing dependence on inherently unstable men and regimes."[30]

The original policies of the CIA were to stabilize Western politics in favor of the United States as much as possible during the postwar period, while at the same time destabilizing and removing any elements that could threaten economic reconstruction and the political stability that it was intended to bring. The CAS was used extensively in support of this; however, by 1954 with the consolidation of American power in Europe—and the full development of the paramilitary capacity of the CIA—the agency turned its focus onto the developing world.[31] The shift of

focus from Eastern Europe to the underdeveloped countries during the 1960s was due to, first, the establishment of the Iron Curtain and the Berlin Wall, lessening availability/opportunities to use classical forms of intelligence collection, leading to heavier reliance on electronic intelligence; and second, the general development of increased activity with policies in developing areas and the shift from a Soviet/Chinese focus to one on the developing world.[32] Furthermore, following African decolonization, CIA activity in Africa increased 56 percent (1959–63) due to fears of Soviet encroachment on these newly independent states.[33]

This shift in focus to the developing world was not solely due to the emerging Cold War confrontation there; it was also a continuation—indeed, reinvigoration—of previous American (and other powers') neocolonial interests in these countries. The 1953 joint CIA–Secret Intelligence Service (U.K.) operation in Iran in support of the shah (and, in turn, his support for the Anglo-Iranian Oil Company) and the 1954 operation in Guatemala (which attempted to use (once again) the United Fruit Company as a covert conduit for intervention, which ultimately was rejected by the company) both exemplified perfectly the growing interlinkage that the United States and other Western powers feared between socialist/communist movements and the efforts of decolonization (including its associated moves to "nationalize" strategic assets previously owned by Western companies, alongside other politico-economic moves that disturbed Western intelligence services and their political masters. Given the assistance that the Soviet Union rendered to these "national liberation" movements, one can find the central interests of Western intelligence in the 1950s and 1960s at this crossroads between the West's attempts to forestall or otherwise control the decolonization process while conducting similar efforts to confront the spread of Soviet influence and interest in the developing world.

These shifts also resulted in the aforementioned overall change in focus and mission of the CIA from an agency dedicated to intelligence collection and counterintelligence actions against its main adversary (the Soviet KGB and its satellite services) to an agency focused heavily on covert actions throughout the developing world—most of these the general (or even specific) continuation of the twin U.S. policies of noninterference and intervention practiced from the nineteenth century onward. The diachronic growth of covert action has been relative to the rapid growth of other aspects of foreign policy implementation due to the leading role the United States has played on the world stage since 1945. As successive presidents have been presented with the opportunity to use this quiet option rather than the other means of intervention, its very use increased immeasurably the number of times it would have to be used.[34] This self-perpetuation is just one of the problems that exist—the other being how successfully congressional oversight has ensured both adherence to mandates by the agencies involved and the accountability of the executive in authorizing covert actions.

In 1975—known as the Year of Intelligence, in which the U.S. intelligence community (and most particularly the CIA) were labeled as a "rogue elephant on the rampage" by the congressional Church Committee, investigating a growing

succession of revelations relating to illegal covert activities conducted overseas by U.S. intelligence and military agencies (many dealing with the assassination of foreign nationals and leaders)—Congress moved to regain control over these activities. Starting with the 1974 Hughes-Ryan Act, which established a law requiring the reporting of secret arms sales and covert actions to the congressional intelligence review committees, Congress passed its own succession of legislation attempting to control such operations—including the 1980 Intelligence Accountability Act and the 1982 Boland Amendment.[35] However, as was evidenced by the Iran-*contra* arms dealers, who found their way around even these types of stipulations, serious flaws may continue to exist in the safeguards established to prevent such things from occurring.[36]

Soviet Covert Action Development

In the case of the KGB, the Soviet intelligence services were carrying out such actions since the time of the Russian Revolution (such as the noted example of the Trust). Covert activities—clandestine political action in particular—were considered to be "the central thrust of the Kremlin's [foreign policy] . . . the leaders' prime executor of such policies is . . . the KGB."[37] From 1945, the United States was referred to as the "main adversary" of the KGB, a designation indicating the main focus of all activities, and as such policies were designed to take this into consideration.[38] KGB goals were not laid out as clearly as those of the CIA, but their aims do not seem to differ that much: generally an effort to influence the world toward a policy of friendliness for their parent state. Where they did differ was in their actions and aims against communist dissidents, defectors, and other threats to the continuation of the global communist revolution.

The KGB became the main arm of the Kremlin in dealing with both world communism and communists around the world. On the former, it justified the control it exerted over all aspects of international communism (client regimes, front organizations, proxy armies, etc.) by stating that "to ignore the activities of international progressive public movements . . . may isolate and weaken national revolutionary forces . . . fraught with the danger of defeat."[39] On the latter, it used its international reach to undermine and if necessary silence those from the East Bloc communist countries who had defected or otherwise organized external opposition to the supremacy and longevity of the Soviet state.

Soviet interests were essentially the same as in the West: a desire to establish influence throughout as much of the globe as possible. In the 1940s and early 1950s, these activities were focused on Europe. But like the CIA, the KGB shifted its focus to the developing world during the 1950s and 1960s, attempting to establish influence in this uncultivated area. One of the most significant defectors to the CIA throughout the course of the Cold War, Anatoli Golitsyn, stated that in 1959 the KGB's primary mission had changed from conventional espionage to "covert statecraft": the use of agents and other mechanisms to achieve geopolitical goals.[40] One final aspect of the relationship between the KGB and its

proxies was that the KGB was itself the sword of another organization, the Communist Party of the Soviet Union (CPSU). All actions the KGB undertook internationally throughout the period were coordinated with the International Department of the Central Committee of the CPSU; the KGB was the conduit for implementing the internationalist policies of the party. The main branch of the KGB that carried out these activities was Department D (later Service A) of the First Chief Directorate; this department coordinated action directly with the International Department.[41] Much of this emerged out of the prewar policies of the COMINTERN: developing international organizations with the "basic aims of promoting the national Communist parties, propagating the Soviet line, and developing political forces subservient to Moscow."[42]

EXAMPLES OF COVERT ACTIVITIES

Propaganda and Psychological (Information) Operations

Propaganda—often referred to as psychological warfare/operations or *psy ops*—is a broad category under which a wide range of information operations can be undertaken. As part of what he refers to as "political warfare" (i.e., statecraft and covert action), Janowitz defined propaganda as "the planned dissemination of news, information, special arguments, and appeals designed to influence the beliefs, thoughts, and actions of a specific group."[43] Focused generally on activities undertaken as part of both covert and overt action—with corresponding deployment of white and black propaganda—it is often deployed in conjunction with other covert activities (e.g., covert political action) and with a wider aim than simply to propagandize. It can include activities in peacetime (such as benign government spin or malign persuasion activities) or wartime (such as military communications operations, cyber or "information" operations, or active psychological operations on both the tactical and strategic levels). A good example of such activities would involve leaks to various press outlets, either friendly (Western) or national outlets within the target country, in which a certain story or approach to a story is conveyed—for example, a pro–United States or pro-Soviet story in a country where the government opposes said power. Through this medium, native citizens can be seen to be supporting a particular U.S. position contrary to their own government, with the intended outcome often being the aiding or debasing of foreign political figures.[44] In one way, this is nothing new in the twentieth century: in a June 1853 article in the *New York Tribune* titled "The Russian Humbug," Karl Marx discounted widespread European press reports of Russian troop movements toward the Balkans as "nothing but so many ridiculous attempts on the part of Russian agents to strike a wholesome terror into the Western World."[45]

One key aim of propaganda is "persuasion": a term encompassing issues broader than simple propaganda, persuasion may be a mixture of threats and appeals which include a large element of spiritual or physical coercion and

violence. This can include the use of bribery, blackmail, and the threat or application of such physical acts of violence as kidnapping, torture, and the use of "controls" over selected targets or agents. In this sense, "persuasion" is directly linked to what Allen Dulles described as the primary interests of "clandestine intelligence collection"—or espionage.

These activities were practiced equally by both Superpowers during the Cold War: in the 1950s, the US established a Psychological Strategy Board directly responsible to the President.[46] The Soviets subscribed to the same principle: "persuasion first, coercion afterward."[47] The media was used extensively in this pursuit by the CIA, the KGB, and virtually all any other intelligence service who wished to promote a particular view. The policies behind media usage were clear: general propaganda and support of one's own policies were the goal. To achieve this, the CIA used

> networks of several hundred foreign individuals . . . who provide intelligence for the CIA and at times attempt to influence foreign opinion through the use of covert propaganda. These individuals provide the CIA with direct access to a large number of foreign newspapers and periodicals . . . press services and news agencies, radio and television stations, commercial book publishers, and other foreign media outlets.[48]

For the KGB, a distinction was made between propaganda and disinformation: propaganda was described as "directly attributed to the Soviets, the satellites, the client states, or the obviously predisposed," whereas disinformation was "seldom attributable to these sources and depends on its false attribution to an ally, to 'discovered' classified documents that purport to reveal plans to attack the USSR and to other rumors, forgeries and orchestrated deceptions with enough verifiable content to raise serious doubts among allies."[49] Irvine has pointed out, half-jokingly, that "the extension of Communist control over vast areas and populations since the end of the Second World War has owed more to the propaganda and disinformation offensive of the Communist countries than to the power of their arms."[50]

While Radio Free Europe/Radio Liberty—established in 1949 and 1951 respectively, and run by the CIA until the early 1970s—operated overtly,[51] the hand of the U.S. government was covert, as it was assumed that they would "be more effective if the role of the [USG] was not apparent."[52] Other examples of CIA use of radio propaganda include the Voice of Liberation radio used during the coup in Guatemala in 1954;[53] Radio Nejat (Liberation) out of the "Front for the Liberation of Iran" to which the CIA reportedly paid $100,000 per month in 1982;[54] and Radio Swan, established under the Gibraltar Steamship Corporation in Miami, against Cuba from 1960 (this later became Radio Americas and Vanguard Service Corp., respectively, after the Bay of Pigs invasion) until 1969.[55]

The KGB never used radio to the extent the CIA did but preferred to carry out its active measures in disinformation and propaganda through surrogates in the communist world and by influencing the print press. The aim behind such

usage was as noted: propagating the Soviet line, encouraging negative reactions to their opponents, and recruiting and developing agents. This was done through a number of methods, the primary of which was the planting of *dezinformatsia* in neutral papers either knowingly or unknowingly. An example of this was the late 1960s reporting of the use of bacteriological weapons by the United States in Indochina in the Bombay *Free Press Journal*. This story was picked up by the *Times* in 1968, as well as other Western print media.[56] Another example was London's *New Statesman*, which was unwittingly used in November 1982 to discredit U.S. Ambassador to the United Nations Jeane Kirkpatrick by linking her with South Africa's infamous security police and South African military intelligence.[57] A final example is the use of the media to better leaders' images: stories picked up by *Time* and *Newsweek* during Andropov's tenure as chairman of the KGB stated that he was "a closet liberal" who "speaks English well . . . collects big band records and relaxes with American novels, [and] sought friendly discussions with dissident protesters."[58] The KGB also used press agencies as fronts extensively—such as the Novosti Press Agency, which acted "as one of the vehicles for Soviet 'active measures'—both for the promotion of stories and to act as 'covers' for KGB officers abroad."[59] Finally, individual journalists—such as Danish journalist Petersen who was directed to attack the British Conservative Party, Thatcher, and other anti-Soviet elements in British politics between 1973 and 1981 through pamphlets and articles either written by himself or by Service A under his name[60]—to push the party line covertly. Indeed, Barron states that out of the approximately 500 Soviet journalists abroad at any given time during the later Cold War, although the majority were intelligence officers, the minority (who weren't free to travel outside of the Soviet Union without KGB authorization) could not refuse a request by the KGB to carry out an assignment.[61]

The CIA used similar methods, but not to the same extent. In 1953, Allen Dulles expressed the desire to use the press for both intelligence collection and propaganda.[62] However, rather than doing so blatantly, the CIA relied on U.S. journalists who would want to "help their country,"[63] maintaining a vast network of reporters, magazines, electronic media, and other media personnel to supplement official information to promote current U.S. policies—including covert propaganda and psy ops—through quiet channels.[64] Though most did so unknowingly, the CIA did use journalists directly—both American and foreign nationals—in "clandestine relationships of one sort or another" with the CIA.[65] Carl Bernstein claimed that more than 400 U.S. journalists secretly carried out CIA activities from 1952 to 1976. The Church Committee stated fifty for the same time period, CIA official sources suggest thirty-six.[66]

Finally, the CIA also funded and covertly supported newspapers, journals, and other print media around the world. Some, like its funding of *Der Monat* (FRG), *Encounter* (U.K.), and the *Daily American* (Rome),[67] was within the context of direct rivalry with the Soviets. Others, like *El Mercurio* (Chile) and *Elimo* and *Salongo* (Angola),[68] were to promote CIA interests in a specific region of the globe in support of other operations—for example, during the Vietnam

War, the CIA allegedly wrote whole articles for *The Economist* on the war.[69] Last, numerous books were published with covert CIA funding and support—including *The Dynamics of Soviet Society* and *The Foreign Aid Programs of the Soviet Bloc and Communist China*.

Covert Political Action

The second and perhaps most extensively used form of CA is *covert political action* (CPA). Treverton defined CPA as "attempts to change the balance of political forces in a particular country, most often by secretly providing money to particular groups."[70] Blackstock further broke down CPA into three stages: *infiltration-penetration*, *forced disintegration*, and *subversion-defection*. Infiltration ("the deliberate/planned penetration of political and social groups within a state by agents of an intervening power for manipulative purposes") as well as subversion ("the undermining or detachment of the loyalties of significant political and social groups within the victimized state, and their transference, under ideal conditions, to the symbols and institutions of the aggressor") are the most relevant here.[71]

CPA has often provided the central desired outcome in a covert action where other activities—such as paramilitary or propaganda activities—have also been deployed. In some senses, therefore, CPA can be seen as the strategic covert action (encompassing propaganda/disinformation, direct political influencing, paramilitary support, and use of social organizations where related to the Cold War confrontation) and other activities intended on attaining a political outcome.

CPA has been conducted both directly by the state seeking an intended outcome and by proxy or partner organizations working on behalf of the state. The latter have taken many forms: for example, both the CIA and the KGB attempted to influence political parties throughout the world in an effort to directly or indirectly undermine the influence of the other, as well as to further consolidate U.S. or Soviet interests in a region. Social organizations, such as student groups, international front organizations and legitimate bodies, and proxy armies were founded, penetrated, and funded by both services. Media outlets, individuals, and services were utilized either knowingly or unwittingly by the CIA and the KGB. Various corporate organizations or services were used as fronts for CIA or KGB activities across the globe. Finally, individuals fell prey to or were used by such activities in such gambits as false-flag recruitments, the deployment of agents of influence, and the role of defectors and disinformation agents in both Cold War camps.

PERSUASION AND INFLUENCE

Blackstock refers to this as manipulative persuasion or control, in which—in the pursuit of intelligence collection activities—the source is controlled or made

dependent on his handler through payment in money, goods, drugs, sex, or other perquisites. The latter activity included the use of first- and second-level agents (targets and people with access to the targets) for manipulation and control, as well as the use of bribery or "quiet assistance," as William Colby referred to it. Such activities were nothing new for the United States (as with other powers). Bribery had been used extensively as a form of persuasion for centuries. In the first U.S. congressional appropriation act in 1789, a contingent fund for the bribery of foreign statesmen in the pursuit of American national interests was approved as part of the public purse.[72] More recently, recipients of funds as part of these activities reportedly included the Christian Democratic Party of Italy, King Hussein of Jordan, and various pro-Western factions in Greece, Germany, Egypt, Sudan, Surinam, Mauritius, the Philippines, Iran, Ecuador, and Chile.[73] The influencing of elections—especially in Western Europe, where the United States pushed the opening of Europe to ensure the development and continuation of economic reconstruction along friendly lines—was a prime CPA activity; indeed, Treverton states that these election projects became central to all nonmilitary CA in the future.[74] CPA was developed even further under Dulles in the 1950s: his personal interests in securing democracy against the Soviets in Eastern and Western Europe led to a dominance of CPA during the 1950s, with direct influence on parties and politicians in Western Europe,[75] which continued over the years.

Case Study: Italian Elections and CIA Funding

Italy provides the best example of the use of CPA funding to influence elections. Beginning with the 1948 Italian elections, in which the CIA funded heavily the Christian Democrats, between 1948 and 1975, over $75 million was spent by the CIA on Italian elections, $10 million for the 1972 elections alone. The CIA reportedly funded over $1 million to Amintore Fanfani, the secretary-general of the Christian Democrats, in the 1970 elections; at the same time, over $800,000 was given to Gen. Vito Miceli, leader of the neofascist MSI and former head of Italian military intelligence, to ensure success. Even following the Church Report (1976), President Ford approved an additional $6 million for the next election.[76]

The CIA was most often the instrument used to provide clandestine support to such parties and states not only because of its black budget, which allowed for expenditures without justification (unlike, for example, foreign aid budgets) and meant that often the recipient might not even be aware of from whence the funds derived. Finally, it also provided the U.S. government with the all-important plausible deniability should such activities come to light.[77] Other states/parties that received such extensive support included the new Federal Republic of Germany and its Christian Democrat Party (and, reportedly, the Social Democratic Party), as part of wider CPA efforts in West Germany to establish or revive

anticommunist, pro-American institutions, discrediting and destroying leftist opposition movements.[78] The Christian Democrats—favorites of the CIA around the world—were also supported in Portugal following the April 1974 coup.[79]

The KGB was also active in this regard. In general, foreign Communist Parties were used as auxiliaries by the KGB as well as recruiting grounds in foreign countries (there is no evidence found to indicate that the CIA recruited within these Communist Parties, although logically this would have often been the case).[80] For example, a great deal of the activities of the French Communist Party were directed from Moscow and were used as a means of penetrating the French government.[81] Moscow Centre's instructions to its stations in this regard states that the main thrust of active measures were to achieve political influence and penetration, such as in Denmark.[82] Overall, although there is indication of attempts made to influence the socialist parties in Western Europe, in general (with the possible exception of the British Labour Party) there has been little success by the KGB in influencing any noncommunist party in Western Europe.[83]

In the developing world, the use of political parties was significantly different. Whereas in Europe, influence over political parties was carried out purely along ideological lines, in the developing world a different pattern emerged. It appears that the CIA operated under the belief that if a party was not aligned with Washington and was not helped along toward that end, then it would automatically fall into Moscow's camp. As is clearly evident with hindsight, nothing could have been further from the truth; indeed, as the example of Castro in Cuba in 1959–60 provides, there were clear cases where such parties were scorned by the CIA or even pushed into the KGB/Soviet camp through CIA action/inaction. Prados refers to these CIA-supported parties as "third force" political movements—generally noncommunist (preferably anticommunist) but also not fascist and politically moderate (usually Christian Democrats). In Latin America, they were usually associated with established oligarchies and in Africa and Asia with tribes. In instances where no third force existed, one was created: examples include the Committee for the Defense of National Interests (Laos), Committee for a Free Albania, Holden Roberto in Angola, and Mobutu Sese Seko in the Congo. The problem that emerged with these groups was that usually, such minorities did little to satisfy general, popular aspirations and often led to further upheaval and, as in Laos, additional obligations for U.S. support. They were generally perceived as "agents of American power."[84]

Case Study: The CIA in Chile, 1963–74

The most obvious case of CIA involvement with developing world political parties is that of Chile. Overall political control and penetration was attempted through the Organization of American States to legitimize U.S. anticommunist actions throughout the hemisphere but was largely unsuccessful. But in Chile, after fears that Allende would become another Castro for the United States to deal with, a psy ops action was authorized that started in 1963 and lasted until

Allende was deposed in 1973. Consequently, the CIA intervened in every election in that time. During the Popular Unity coalition government in Chile, the Christian Democrats and the National Party were funded with over $4 million from the CIA; at the same time, monies were used to attempt to lure away factions from the coalition. In 1964, $2.6 million was given to the candidate Frei (who later won) to prevent Allende and the socialists from gaining power.[85] The United States also spent—through the CIA, supported by various private corporations (such as ITT) with business interests in Chile—$12 million to blacken Allende's name.[86]

On its side, the KGB generally helped communist and socialist movements in the developing world, but almost without exception only when they were linked to paramilitary formations involved in war. One clear example is that of the Popular Movement for the Liberation of Angola (MPLA), supported by the KGB until 1974, when Cuba became their prime supporter at the time of the Portuguese coup. This was against not only Jonas Savimbi's South African– and CIA-backed UNITA but also (as noted) Holden Roberto's CIA-supported National Front for the Liberation of Angola (FNLA), the largest anticommunist party in that country.[87] This provides the perfect (and perhaps best) example of a developing country where at least three sides were supported against each other (and their benefactors) to the detriment of the country and its citizens. In Afghanistan, the head of the dominant faction in the Afghan Communist Party, Babrak Karmal, was a KGB agent. Moscow Centre was also reported to have a number of agents directly in Nasser's entourage, including Nasser's head of intelligence.[88] Finally, Andrew and Gordievsky state that the African National Congress (ANC) was greatly penetrated by the KGB due to the ANC's close links with the South African Communist Party, itself deeply tied to Moscow.[89] Finally, a strong example of CPA activities by a Soviet satellite is the extensive operations conducted by Markus Wolf's Foreign Intelligence Division in the East German Ministry for State Security (or Stasi) against the West German government in Bonn (as well as business circles throughout West Germany) over many decades of the Cold War, resulting in the resignation of West German Chancellor Willy Brandt in 1974 after his private secretary was exposed as one of Wolf's moles.

In general, though, neither the KGB nor the CIA were very successful in their usage of political parties in the developing world. The United States and, to a lesser extent, the Soviet Union failed to understand the nature of developing world socialist movements and their links to international ideologies. As already stated, the end result more often than not was additional problems for the individual service, whether on a massive scale such as Indochina and Afghanistan or on a smaller scale such as Central America or Angola. As Prados states, one of the problems of working through proxies is that of suffering political liabilities as a result of acts by such allies, as well as the obvious one of lack of full or even sufficient control over these allies. Examples of such problems would include the

drug smuggling carried out by the Indonesian military regime, Li Mi's Chinese, and Vang Pao's Meo.[90]

FRONT ORGANIZATIONS

The extensive development and use of front organizations by both the CIA and KGB—as well as other intelligence services, such as the Israeli Mossad and the apartheid South African National Intelligence Service and Police Security Branch—provides some of the best examples of covert political activities. Some such fronts include the proxy-ized political parties noted above, but the truest of such organizations were those without apparent linkage to any foreign government.

The use of front organizations by both the CIA and KGB was widespread throughout the whole of the Cold War. These organizations took on different guises depending on the requirements of the period, the intended action, and the hoped-for outcome. In the case of the CIA, however, the vast majority of these fronts were direct appendages of the agency. The CIA's policy was to base its support on a wide range of groups and institutions (besides political parties) in various countries to "shift the balance of that country's politics by countering groups perceived as threatening to American interests and aiding those friendly to the United States."[91] In the case of the Soviets, the KGB often acted as a filter for other Soviet organizations (primarily the International Department of the CPSU); therefore, even in instances where a front was not a direct arm of the KGB, it was linked through the committee to other organizations.

For the Soviets, who had established the use of fronts with the GRU (Soviet military intelligence) in the 1920s to obtain monies and economic considerations without it being apparent that these were going to the Soviet Union,[92] their policy was articulated in the March 1926 statement from the Comintern advocating "creating a whole solar system of organizations and smaller committees around the Communist Party . . . actually working under the influence of the Party, but not under its mechanical control." The overall task of these fronts were to "advance the cause of Soviet Communism, to defend the policies of the Soviet Union . . . and to attack the policies of those it opposes." They were also used to recruit agents, provide covers for illegals, and "mould and manipulate public opinion."[93] Most of the fronts that the Soviets used during the Cold War were legitimate in their founding but were captured by the Soviets during the period from the 1920s until 1950.

The CIA's approach to fronts was generally to use a variety of corporate fronts, usually referred to as either "proprietaries" or "Delaware Corporations,"[94] which took many different guises and forms throughout the Cold War, depending on geography, mission, and time. Indeed, it could be argued that the post–Cold War growth in private security and military companies operating internationally—and the role that they fill not only for their client governments or corporations in the Developing World but also in the contracts that they undertake on behalf of Western governments—are a direct descendant of such organizations However,

throughout the Cold War and as far back as the U.S. government's use of Vinnell Corporation in Mexico in the early-1930s and throughout World War II (later described by a CIA official as "our own private army in Vietnam"), such private security and military companies provided the same type of service that was secured through these fronts, under very similar circumstances of plausible deniability and ease of use far from the public's eye.

The most well-known type of proprietary was the air corporations. These were established (generally) during the wars in Indochina and in relation to the conflict between Formosa (Taiwan) and communist China; the best known of these was Civil Air Transport (CAT),[95] used in operations involving Li Mi's Nationalist Chinese forces, as well as in support of the French in Indochina, and Air America, which emerged out of the CAT experience and the desire for an International Volunteer Air Group in Southeast Asia.[96] Double-Chek Corporation, listed as a brokerage firm in Florida government records, was in reality a recruiting front for pilots flying against Cuba after 1959; many of the pilots flying B-26s out of Central America against Cuba were recruited by a company called Caribbean Marine Aero Corp. (Caramar), a CIA proprietary.[97] More recent examples include Summit Aviation, which was linked to the CIA during the 1980s with operations in El Salvador and Honduras;[98] and St. Lucia Airways, which, although they deny it, was conclusively tied to the Iran-*contra* operations (along with several other such fronts) as well as to operations in Angola and the Congo (Zaire).[99]

Other types of fronted activities include the use of United Business Associates (Washington) to fund corporate development in the developing world to "offset the Communists from moving in,"[100] and—as a direct continuation of previous U.S. activities—the CIA was supported by the United Fruit Company in developing plans to carry out the 1953 coup against Arbenz in Guatemala, but it never followed through.[101] Finally, one of the best known front organizations of the CIA was Zenith Technical Enterprises, a Miami-based corporation used to organize, direct, fund, and carry out Operation Mongoose, the CIA's war against Castro.[102]

In contrast, no evidence was found to indicate that the Soviets, having pioneered the corporate front with Arcos (All-Russian Cooperative Society, officially the Soviet trade mission in London but in reality the cover for extensive industrial and commercial espionage) in 1921 (and subsequently smashed by MI5 in 1928),[103] continued with corporate fronts after 1945.

South Africa engaged heavily in all manner of covert activity during its wars against the anti-apartheid movements, both in Southern Africa and further afield. Its best-known police intelligence operative—Craig Williamson—was also one of its most successful in conducting CPA operations against the worldwide anti-apartheid movement, particularly in its strongholds in London and Western Europe. In 1972, Williamson, along with Craig Edwards, successfully infiltrated the ANC's structures via the International University Exchange Fund based in Geneva (of which Williamson eventually became deputy director), redirecting

virtually all of its fundraising income into South African government secret accounts. He returned to South Africa only after being exposed in 1980, having run the operation for eight years.[104] Indeed, over the course of the 1960s through the 1980s, a triangle of covert support and activities developed between the CIA, South African intelligence, and Israeli intelligence—with British and French intelligence and Zaire's Mobutu sitting somewhat uncomfortably on the edge of the triangle—to confront Soviet/Chinese/general communist influence in Africa while ensuring access to strategic resources.

The CIA also used social and educational organizations—such as the National Student Association, which the CIA had funded (to 80 percent of their budget) between 1952 and 1967 in an attempt to counter Soviet efforts to mobilize world youth,[105] or the European Market Movement to which the CIA provided £380,000 between 1947 and 1953 in an attempt to directly balance KGB activities in the same manner.[106] Finally, anticommunist trade unions were heavily funded by the CIA in Europe and the developing world.[107]

On the Soviet part, Lenin first introduced the idea of propagating communism through trade unions, youth organizations, and other social groups in 1921;[108] over the proceeding years, hundreds if not thousands of Soviet front social organizations existed. Most emerged initially out of Willi Münzenberg's "Innocents' Clubs" of the 1920s where individuals were recruited to the communist cause;[109] since 1945, these have been more concerned with rallying specific social groups across the globe. In 1965, there were eleven official such fronts—such as the World Federation of Trade Unions and the International Union of Students—linked to the Soviet Union.[110] Regionally, such organizations as the Nigerian Trade Union Congress and the Afro-Asian People's Solidarity Organization were funded and utilized by the KGB.[111] The largest such social front was the World Council of Peace/International Institute for Peace, expelled from Paris in 1951 for "fifth column activities," then from Prague to Vienna, where it was banned in 1957 for "activities directed against the interest of the Austrian state," finally establishing itself in Helsinki in 1968.[112] It is believed to have received over $50 million annually through the KGB and even achieved recognition from the United Nations and UNESCO.[113] Finally, although often claiming responsibility for encouraging peace movements (such as the Campaign for Nuclear Disarmament responsible for the protest at Greenham Common), KGB aid could not have motivated them any further, according to Andrew, as they were already in the 1980s very intensely anti–United States.[114]

Covert Economic Action

The third form is *covert economic action*. This includes the attempt, through covert means, to disrupt or destabilize adversaries' economies. Methods used have included counterfeiting foreign currencies, depressing the world price of agricultural products vital to adversaries (especially one-crop developing nations), trying to control the rainfall over enemy territory through cloud seeding,

preparing and introducing parasites for the destruction of crops, contaminating oil supplies (as was done against North Vietnam), dynamiting power lines, and mining harbors to discourage commercial shipping (as Reagan authorized against Nicaragua).[115]

Covert Paramilitary Action

Finally, the fourth method encompasses both covert paramilitary action (PM) and counterintelligence[116]—or what are collectively sometimes referred to as "secret wars." These include all manner of assassination, coup, raid, counterguerrilla activity and other (generally) armed covert acts. Charters states that these "involve the active direction, deployment, or support of regular or irregular armed bodies of men employing unconventional military means to achieve their (or their sponsor's) political objectives." In this sense, Charters maintains that these activities are closer to military special operations—fitting, given that military special forces and their missions often form part of covert PM actions.[117]

The first American covert PM involved the only time in which the United States engaged in *direct* covert military activities against the Soviet Union—the CIA's (and U.S. military Counterintelligence Corps in occupied Germany) support for anti-Soviet Ukrainian partisans in 1947–48. After that time, the United States did not take direct PM activities within the Soviet Union (unlike, for example, its support for the Afghan *mujahedeen* during the Soviet-Afghan War).

Throughout Africa during the Cold War, the CIA supported Mobutu in the Congo as both a bag man and staging point for all manner of covert paramilitary (and other) activities in Africa—including extensive covert cooperation with apartheid South Africa within the anticommunist Cold War context. The Soviets parried by providing extensive support (alongside and often in competition with the Chinese) to the liberation and revolutionary guerrilla movements across the continent—including especially in Angola, Mozambique, Rhodesia/Zimbabwe, and South-West Africa/Namibia. This, in turn, generated further South African–Rhodesian covert efforts to undermine these revolutionary guerilla movements using their own panoply of covert activities (including the extensive use of assassinations, pseudo-operations, third-force [proxy] counterguerrilla forces, and the like)—creating a spiral of covert action-reaction across the breadth of central and southern Africa throughout the 1970s and 1980s.

In Latin America, covert paramilitary activities against Castro and in Chile, Guatemala, Nicaragua, and El Salvador—culminating in the Iran-*contra* scandal of the 1980s—witnessed the continuation of U.S. interventionist policies from the last century. In Vietnam, initial covert assistance to the French during their Indochinese campaign evolved slowly into the CIA's biggest "war" by the mid-1960s, culminating in the PHOENIX Project. Outside of the Cold War context, the 1985 French special services attack on the Greenpeace *Rainbow Warrior* in Auckland harbor symbolized other aims of covert activities (in this case, acting against a group actively protesting nuclear testing in the South Pacific).

Case Study: Nicaragua, 1933–87

The most well-known example of transition from direct to indirect control is the case of Nicaragua. Before pulling the armed forces out of Nicaragua in 1933, the United States trained and equipped the National Guard, whose leader, Anastasio Somoza, instigated a successful coup in 1936. After maintaining very close ties, in all aspects, with the U.S. government for forty-six years, the Somoza government was overthrown in a revolution led by the Sandinistas in 1979. The funding of the National Guard, now called the *contrarevolucionarios* (contras), continued by the CIA from 1979 until it became public in 1987.[118]

At their height in the United States in the 1980s, the combination of both PM and CI authorizations—Reagan's 1981 Executive Order 12333—was the basis for CIA foreign activities under the Reagan Doctrine. As is noted, however, it was long before that the United States developed and deployed its covert paramilitary capability under the Cold War rubric.

The United States was no stranger to counterintelligence operations, having performed their first ones under the Committee of Secret Correspondence, established by George Washington in 1776, against British agents in New England. The first covert action carried out by the U.S. government (in conjunction with France) was the funding of arms to back a coup in Tripoli to place a ruler friendlier to the United States on the throne.[119] But as a prelude to U.S. actions two centuries later, these were child's play.

PM action primarily involves the support of guerilla and other insurgent groups against governments unfriendly or threatening to the United States. For example, from 1963 to 1973, the CIA supported the Meo tribesmen in Laos against the communist Pathet Lao government. Other countries where this type of CA has reportedly taken place include Ukraine, Poland, Albania, Hungary, Indonesia, China, Oman, Malaysia, Iraq, the Dominican Republic, Venezuela, North Korea, Bolivia, Thailand, Haiti, Guatemala, Cuba, Greece, Turkey, Vietnam, Afghanistan, Angola, and Nicaragua, to mention but a few.[120]

These operations were historically carried out jointly by the Directorates of Operations and Administration (responsible for training and support). As well as insurgent support, the CIA has funded various PM training activities throughout the world, provided military advisors (as in Vietnam before full-scale military deployment, and in the recent Afghani war against the Soviets) and transported arms shipments internationally to supply pro-U.S. factions world wide (such as the delivering of Stinger and Blowpipe missiles to the Afghan *mujahedeen* resistance during the 1980s Soviet-Afghan War).[121] Much more recently, as the first U.S. government activity directly against the Taliban and its Al Qaeda supporters in Afghanistan before and during Operation Enduring Freedom, the CIA deployed the "Jawbreaker" team as a covert PM activity aimed at supporting the Afghan Northern Alliance against these foes to foment direct action against them.

As an issue that—like others—intersected CPA and covert PM action, the instigation of physical terror, kidnapping, and assassination serves a double purpose. While political opponents are temporarily or permanently removed from the scene, violence itself is used to create fear and hatred, often discrediting or undermining one entity against another. This is what Blackstock has referred to as "the essence of forced disintegration or atomization," by which the political and social structure of the state is split apart. This use of "executive action" (more commonly referred to as assassination) is something that the CIA has never admitted to, but it is known that several attempts were made on Castro, either by CIA personnel or by CIA-backed assassins (such as the Mafia).

Less well-known, however, are the attempts (and successes) at lower-level assassinations (not prime political figures)—with paramilitary operations such as the PHOENIX Project in Vietnam (see later discussion), the promotion of selected targeting or extrajudicial killings through the School of the Americas at Fort Benning, and other initiatives aimed at decapitating revolutionary or guerrilla movements at the command-and-control level. The death squads run throughout Central America by the CIA during the early 1980s followed similar lines.[122] Following the 1975 Year of Intelligence revelations in the United States and moratoriums on "assassination" initiated by Presidents Ford and Carter, section 2.11 of Executive Order 12333 now prohibits this.

Assassination was also a favored practice of the Soviet intelligence services and their satellites—usually conducted against dissidents from communist countries (such as Georgi Markov of Bulgaria, infamously assassinated in 1978 on London's Waterloo Bridge by a lethal ricin dose delivered by a sharpened umbrella) in exile or those who helped support them and their activities. The Israeli government has made extensive use of assassination—against not only its opponents in the Arab world (such as Hamas bomb maker Yahya Ayyash, known as "The Engineer," assassinated by mobile phone bomb in 1996) but also those who were suspected of helping their enemies (such as Gerald Bull, the Canadian designer of the Iraqi super-gun, assassinated in Brussels in 1990). The apartheid South African government made extensive use of assassination as a covert tool furthering state policies, not only within South Africa but across the front-line states of southern Africa and even as far abroad as London, Brussels, and Paris, where members of the ANC and other liberation movements in exile as well as other players in the anti-apartheid movement worldwide were assassinated with extreme professionalism and success. Indeed, as an example of the success of covert paramilitary activities, the apartheid government's use of assassination (alongside other covert activities) was probably one of the best, forcing the ANC to first withdraw their presence (military bases, offices, and representatives) further from South Africa's borders in southern Africa, and, second, both acknowledge an inability to overthrow the apartheid government by force or revolution and seek a negotiated settlement to the conflict as a result. Israel's assassination activities to this day against Palestinian militants would appear to have had a similar success, at the least in eliminating a considerable cadre of

paramilitary technical expertise from among the ranks of the various Palestinian terrorist and militant groups.

Support for paramilitary formations, proxy armies, and similar covert activities followed directly from this: the CIA supported paramilitary formations in Indochina, Angola, Nicaragua, El Salvador, Ethiopia, Afghanistan, and many other regions. The KGB, almost without exception, supported proxy armies in the same areas opposed to the ones the CIA supported. This involved not only direct activities—such as the PHOENIX Program in Vietnam—but also indirect and support activities, such as training. Although good examples of the latter include the training of the GVN police at Michigan State University under a program using USAID cover[123] and the creation and training of Savak (Iranian security service) by the CIA as a means of gathering information on the Soviet Union in exchange for helping repress dissident activity against the shah's regime[124]—the PHOENIX Program represents the best example of this, and probably the most successful CIA covert paramilitary operation ever. Run by CIA-backed South Vietnamese forces against the Viet Cong Infrastructure (VCI), some 20,000 VCI leaders and sympathizers were killed as a result of this program according to Colby. Despite claims that none of them were killed by assassination methods, members of this program have confirmed at least 10,000 assassinations against the VCI. It is never been confirmed whether or not American agents took part as assassins.

The CIA also used Reinhard Gehlen's intelligence network in postwar Germany (called The Organization, the forerunner of the Bundesnachrichtendienst, or BND) to train Baltic émigrés and refugees to carry out paramilitary CA against the Soviets. These groups acted in concert with the Ukrainian partisan groups in operations against the Soviets in Poland, the Baltics, and the Soviet Union. Eisenhower's Task Force C programs in the 1950s had included the development of a Volunteer Freedom Corps, employing cadres of European émigré fighters, as an aspect of rollback. They failed miserably during the late 1940s and early 1950s.[125] Finally, Vang Pao's Armée Clandestine (Meo units including Operation White Star Green Beret forces) was used to combat Pathet Lao forces in Laos. These included the use of Police Aerial Resupply Units (PARU), not to be confused with the Provincial Reconnaissance Unit (PRU) used in PHOENIX.[126]

For the Soviets, use of such fronts was different from that of the CIA. As already stated, use of proxy armies in the developing world was very similar to that of the CIA. The KGB influenced (and often controlled) the armies of client states (such as Cuba, Angola, Afghanistan, Ethiopia) through replicated Soviet political administrations that placed informers throughout the armies' ranks.[127] The main difference between the two services lay in the KGB's use of "friendly" intelligence services. The KGB directly controlled the intelligence and security services of all the Soviet bloc countries, as well as using the intelligence services of client states, such as Libya. This was done to "give distance and deniability in potentially embarrassing operations," as well as to carry out false-flag recruitment.[128] Examples of this would be the KGB's direction to Czech intelligence to "cause conflict and exploit tension between individual countries, even

countries that recently gained their independence."[129] As well, the East German Staatsicherheitsdienst (SSD) was used between 1959 and 1960 as agents provocateurs to try to destabilize West Germany by infiltrating agents into Jewish areas to desecrate graves, spray swastikas on property, and other similar acts. In 1968, the KGB took direct control of Cuba's DGI in a secret agreement with Castro.[130] In international terrorism, although never directly controlled by the KGB, terrorist organizations, such as the Red Brigades in Italy or the Baader-Meinhof Gang in West Germany, were sponsored by Moscow Centre. This was most often accomplished through surrogate intelligence services, such as East German and Romanian secret services. Links existed as well between these organizations and the Palestine Liberation Organization, as well as the Provisional Irish Republican Army for a number of years.[131] No evidence can be found to indicate a similar relationship between the CIA and its allies regarding either of these two categories.

Ultimately, this is the theory and practice of the propaganda of the deed—practiced by both revolutionaries/terrorists and intelligence officials as part of their covert options.[132] However, these activities were not always successful: Mossad estimated that by 1960, Saudi Arabia had already paid out over $3 million in a vain attempt to arrange for the assassination of President Nasser of Egypt.[133] However, Mossad itself was caught in an embarrassing attempt to assassinate Hamas leader Sheikh Khaled Mashal in Amman, Jordan, in 1997 when their assassins not only failed in their direct action attempt but were caught and publicly humiliated by Jordanian police. Mossad has used assassination extensively throughout its existence, not the least of which in its attempts to hunt down and kill every member of the Black September terrorist group responsible for the Munich Olympics massacre.

Covert Action in Perspective

In all of these actions, overlaps can often be found in practice. A number of these have already been noted—indeed, in most covert actions, multiple outcomes either are intended or are the result (i.e., economic plus political, psychological plus economic, or paramilitary and political). It must also always be kept in mind that these actions are deployed both directly by the instigator—the CIA, the KGB, or another government's instrument—and by the proxies which it supports. Propaganda, for example, can be used to effect or delay political change (as the United States did in Western Europe in the early days of the Cold War or the South African apartheid government did against its ANC enemies) or inspire terror (as was done frequently by both fascist and communist regimes worldwide). Conversely, the actual use of terror—sometimes under the guise of covert paramilitary actions—has its own propaganda effect. A prime example of this mixture between propaganda and covert paramilitary activities is the use of what the British government in Kenya called pseudo-operations—whereby covert units of "turned" guerrillas would visit villages to either gauge local support for

the government or the rebels, or (as the Rhodesian and South African apartheid governments conducted to far greater degrees than the British, French, or Portuguese in their decolonization wars) carry out attacks on those villages to make it look like rebels had been responsible.

COVERT ACTION TODAY

Since the end of the Cold War and across the interregnum of the 1990s CA has evolved to some degree. Indeed, some would argue that it has had to evolve, given that the global environment within which it functions has evolved around it. No longer solely aimed at furthering the aims of intervention, control, or subversion, it has been used by various powers to support more altruistic aims, particularly within the new intervention agenda of the post–Cold War world. With an international security regime driven heavily by humanitarian-led concerns over the rule of law—both domestically and internationally—and a far greater (at least compared to the Cold War context) willingness to push peacekeeping and peace-support operations at the international level and through the United Nations, covert action as a tool of statecraft has been used for support. Part of the reason for this forced evolution is not the least because, in the information age—with the spread and coverage of nonstop news—very few activities can occur unnoticed around the world. Though the original intention of covert activities has not changed—even in those situations where the action is visible, let alone when it occurs under the radar, and the hand of the initiating government is not seen in its undertaking—this rise in media scrutiny combined with ever-increasing public accountability drives the intelligence services (at least in the developed world) has made such undertakings a greater challenge for the intelligence services.

This is not to suggest that covert actions have been undertaken through a United Nations or other regional organizational mandate—but rather that individual powers, acting sometimes with this greater altruistic attitude, have supported a far broader target/interest base than ever was the case during the Cold War. Examples of this include the British government's use of the private military company Sandline International to provide covert support to the exiled government of Sierra Leone in 1999 against the horrendous rebels of the Revolutionary United Front. Another case is CIA support—bungled and dropped in 1995—for the Iraqi Kurds against Saddam Hussein's military and intelligence onslaught after the 1991 Gulf War. In the war on terrorism—really started initially by President Clinton in the mid-1990s—the United States had covert operations against terrorist networks and supporters underway in at least eighty countries by September 2001.[134]

This is not to say that the more traditional state-interest activities have not continued. The CIA's bungles in Haiti in the mid-1990s clashed directly with the Clinton administration's declared intentions and activities aimed at restoring democracy (in the form of Jean-Bertrand Aristide) to that troubled country. In its

war with the Chechen rebels, Russia has deployed significant covert paramilitary actions—including especially assassination, but also propaganda and psy ops—against the Chechen rebels, the Chechen people, and (in terms of propaganda) to the outside world. There are even suspicions that Russia's "special services" have conducted pseudo-operations (both inside and outside Chechnya) in an effort to further blacken the reputation of the Chechen rebels.

Probably the best known post–Cold War covert action gone awry was the use of the UN Special Commission on Iraq (UNSCOM) as a cover for CIA and NSA activities in Iraq during the period of international weapons inspections in that country until its exposure in 1998. Greeted with horror and abhorrence, the CIA was vilified for using the United Nations—with its cloak of impartiality and benevolence—as a cover for intelligence activities. The fallout from this operation not only led to the expulsion of the UN weapons inspectors from Iraq but—it could be argued—directly to the 2003 Iraq War.[135] More recently, it has been suspected that the CIA has been ordered to subvert Hugo Chávez's government in Venezuela, much as it did for the better part of a decade against Castro in Cuba and for much the same reasons.

In the war on terrorism, launched following the September 11, 2001, attacks on the United States by Al Qaeda, the known use of covert action has demonstrated the continuation of similar activities from the Cold War period. The use of propaganda—both overtly through media such as Radio Sawa (much like Radio Free Europe in its latter days) and more covertly through attempts to support the promotion of a more understanding and benevolent image of the United States (and the West more generally) across the Muslim world—has seen extensive examination, both by the media and academia. Covert political action, in the form of attempts to influence or support various governments around the world (such as in Pakistan, Uzbekistan, Indonesia, and other regional governments of interest), has continued unabated. The deployment of CIA Counterterrorism Center/Special Activities Division Jawbreaker teams—armed with both Special Operations Forces and suitcases full of cash—into Afghanistan in the weeks before the launch of Operation Enduring Freedom in October 2001 was the best recent example of this continued practice of nurturing and supporting proxy forces (in the form of the Northern Alliance in this case) through covert paramilitary action. Existing concerns over rogue states or states of concern (such as Iran, Syria, and North Korea) in the first decade of the twenty-first century will likely see the continuation of such activities, both within the context of this war on terrorism and in terms of the broad interests of individual states.

CONCLUSIONS: THE USES AND LIMITS OF COVERT ACTION

It is clear that by the 1990s, the mechanisms of covert action used by the United States became more refined but not necessarily more successful. Overall,

the United States achieved more successes—in this pursuit of statecraft and national interests—during the 1898–1933 period than they have since the 1939–45. Success is a relative concept. In terms of achieving hegemony and maintaining it in their chosen sphere of influence, the United States achieved this by 1914 and maintained it until 1933. The period from 1945 to the present has witnessed the attempts by the United States to reintroduce this concept of hegemony throughout the world with, to a large degree, less success comparatively. The clear difference between the two periods was the evolution of these methods from direct political control and full use of military force, to proxy activities and covert operations spanning the globe. Many of these methods have been, in contrast, very successful in the achievement of immediate goals. In the long run, they had considerably less effect.

During the Cold War, the activities of the United States—and other Western powers—were balanced by those of the Soviet bloc. Since the end of that conflict, the concerns of the CIA—and the United States and other Western powers and their intelligence services—have been redirected to countering regional and local instability and collapse, dealing with humanitarian crises, countering regional and local wars through (generally UN-mandated) interventions, and dealing with rogue states, dictators, and the proliferation of weapons of mass destruction and international terrorism. Although individual states' self-interests have continued to drive not only these activities but also more selfish traditional ones, the geostrategic global balance has now shifted—perhaps irrevocably—to the point where the great (at least Western) powers now act with generally global benevolence in their pursuit of their goals. With the additional challenges that the information age presents to keeping covert actions covert, the pursuit of covert action has become more difficult at the same time that the global public demand for states to be "seen to be acting" with altruistic, globally benevolent interests has increased dramatically. Therefore, *overt* action has come more to the fore in the pursuit of those activities that previously would have been undertaken covertly.

This is not to say that all (or any) states have dropped the pursuit of their own self-interests through the medium of covert action. In the case of previously Soviet (now democratic) Russia, the collapse of Soviet communism and the end of the Cold War also meant the end of the general Soviet pursuit of both supporting the advance of global communism and dealing with those of its citizens abroad who dissented from such a view (along with their supporters), especially in terms of the Cold War covert confrontation between the KGB and CIA in the developing world and all it entailed. The end to these activities symbolizes perhaps the greatest change in covert action goals and aims from the Cold War to the post–Cold War periods. Russia today still covertly pursues its interests abroad through not only its civilian but also (more particularly, in some regards) its military intelligence services. Other states continue to use covert action as a tool of statecraft, such as Israel's pursuit of its national security against its enemies, various rogue states' pursuit of the matériel and capability to develop

weapons of mass destruction capability, and China's pursuit of its growing interests globally.

Assessing Success

At the general level, one may say that the CIA was successful in carrying out many of its covert operations; this is because, as Prados points out, with almost no exception, the actions carried out by the CIA forced the Soviets or the Chinese (the specific opponents named in NSC-5412) to respond in kind without escalating to open military confrontation.[136] This is in contradiction to the general record of CIA covert actions that indicate those CA undertaken over time were more often than not failures in the long or short run. At a more specific level, limited operations were never allowed to stay limited due to the aforementioned problem of escalating commitments, the quagmire of covert action. Thus, even though CA in Angola in 1975 and in Nicaragua in 1980 were initially limited activities aimed at preventing the consolidation of a government in the former case and at harassing the regime in the latter case to prevent its continued support of guerillas in El Salvador, they eventually escalated to such a level that failure was inevitable unless the next step (military intervention) was taken.[137] At this level, the CIA had a number of debacles (Indochina, Cuba) as well as number of limited successes (Chile, Western Europe). Propaganda operations had certain successes; Guatemala is one of the most obvious. Even though the CIA admitted in the post mortem that communism was never a threat in Guatemala, there was not even evidence of contacts with the Soviets.[138] But it was these successes that later led to failures or "problems that rebounded in the face of the [U.S. government]."[139] As far as media successes, opponents of propaganda (or psychological warfare) argue that if overt means had failed, it was unlikely that the target would be persuaded by covert use of media organs. The problem of "blowback" is also of concern; information planted abroad finds its way back into domestic press sources, deceiving one's own citizens.[140] The question is raised as well as to why the U.S. I.A. (United States Information Agency) does not carry out the same role in propaganda because its mission is overt and aimed at spreading U.S. views anyway.[141]

At the most basic level, that of assessing operations individually, the CIA comes up lacking. Mistakes were often made in the planning stages, predetermining failure. This was the case in Libya, where the CIA bypassed the best potential replacement for Qaddafi, and in Iran, where no attempts were made to penetrate religious groups prior to the revolution.[142] In funding support to Tibet, Afghanistan, and Indochina, large portions of CIA assistance was soaked up while still in transit due to corruption. And in some operations, follow-up support could not be granted for various reasons. The most evident case of this was the link between Radio Free Europe (RFE) and the Hungarian uprising in 1956. RFE made vague hints about Western assistance to students and workers in Budapest prior to the revolt; however, once the uprising began, RFE was forced to sit

helplessly and listen to broadcasts from Budapest describing the slaughter. An estimated 30,000 died in the Soviet suppression.[143]

On the Soviet side, in many areas successes were more apparent than with the CIA. The use of paramilitary fronts in Eastern Europe linked to deception operations in the years following the war forced the CIA to establish a Counterintelligence Staff (under James JesusAngleton) in 1954 to counter such KGB operations.[144] At the general level, social fronts were by and large successful in that they forced the CIA to always react, one step *behind* the KGB. The KGB's use of the World Council of Peace (WPC) was very successful in coordinating world opinion, through its leadership of the other social fronts, against the United States during the Vietnam War. But even it ultimately failed in 1989 when it admitted that 90 percent of its funding came from the Soviets.[145] Other perceived successes were in reality distinct from KGB operations. For example, in 1984, the KGB launched an anti-Reagan propaganda campaign using the slogan *Reagan: eto voina!* (Reagan Means War!) during his election campaign. The anti-U.S. reaction to Reagan's victory was claimed by the KGB as a sweeping success; however, the fact that this slogan went unused everywhere indicates another area where the KGB had little to do with world opinion.[146] Where the KGB was successful at this level was in gaining recognition for most of its social fronts by the United Nations, UNESCO, United Council of Churches, and other international bodies. This was largely accomplished through the use of developing world surrogates to influence colleagues and decisions. Furthermore, outside of the known social fronts, many splinter committees, action groups, subsidiary organizations, and the like emerged that carried out much the same work as their parent bodies but without apparent Soviet involvement.[147]

Therefore, it is clear that many similarities and differences existed in the use of covert action during the Cold War—not only as part of the bipolar confrontation but also in unilateral activities by many states. In the case of the United States and the Soviet Union, where the CIA generally dealt with any noncommunist political organizations and individuals that would further their cause, the KGB dealt almost exclusively with communist parties or organizations in an attempt to further world communism. But one could argue that both powers were simply looking out for their own interests and using whatever vehicles necessary to fulfill and secure those interests. Prados has concluded about the CIA that "in all these CIA operations, there is a lesson . . . the United States acts in its own interests, which are those of a Great Power. There is little true identity of interest between the restive local minority and the Great Power."[148] This could easily be said for the KGB and the Soviet Union as well. As far as such fronts are concerned, the Soviets proved themselves much more adept at developing and wielding social fronts internationally than the CIA. The use of the media for propaganda, cover and influence was equally successful on both sides. But where the CIA generally failed in its use of proxy armies, the Soviets can be said to have been successful in their use of surrogate intelligence services and armies to accomplish the spread of the Soviet point of view.

Orwell summed up the raison d'être behind the extensive use of covert action when he opined, "We sleep safe in our beds because rough men stand ready in the night to visit violence on those who would do us harm." However, although the Cold War confrontation saw extensive use made of covert actions to further the aims of an individual service or power, more often than not the interests of that power and the deployment of said covert action acted against the wider global interest. Although the complexities of covert action can be found in Treverton's observation that "secret operations in a democracy are a paradox, all the more so if those operations intervene in the politics of another country,"[149] John Le Carré's observation of intelligence as a barely controlled circus may be closer to the truth of the role of intelligence and the need to stay vigilant over its activities: "Now that we had defeated Communism, we were going to have to set about defeating capitalism, but that wasn't really [the] point: the evil was not in the system, but in the man . . . you want to say: 'I slew the dragon, I left the world a safer place.' You can't really, not these days. Perhaps you never could."[150]

NOTES

1. Although such a vast topic is impossible to tackle adequately within one chapter, there are numerous important academic contributions to be found to this debate within the literature. For excellent discussions of covert action generally—including its uses, links to policy and intelligence, implications, and outcomes—see Paul W. Blackstock, *The Strategy of Subversion* (Chicago: Quadrangle Books, 1964); Loch K. Johnson, *America's Secret Power: The CIA in a Democratic Society* (New York: Oxford University Press, 1989); Walter Laqueur, *A World of Secrets: The Uses and Limits of Intelligence* (New York: Basic Books, 1985); John Prados, *Presidents' Secret Wars: CIA and Pentagon Covert Operations from World War II to the Persian Gulf* (New York: William Morrow, 1996); Gregory F. Treverton, *Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, 1987); Roy Godson, ed., *Intelligence Requirements for the 1980s: Covert Action* (Washington: National Security Information Center, 1981); and David Charters, "The Role of Intelligence Services in the Direction of Covert Paramilitary Operations," in Alfred C. Maurer et al., eds., *Intelligence: Policy and Process* (London: Westview Press, 1985). For studies on the CIA and American democracy specifically, see Loch K. Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (Lexington: University of Kentucky Press, 1985); Frank J. Smist Jr., *Congress Oversees the United States Intelligence Community, 1947–1989* (Knoxville: University of Tennessee Press, 1990); Gabriel Kolko, *Confronting the Developing World: United States Foreign Policy 1945–1980* (New York: Pantheon Books, 1988); Rhodri Jeffrey-Jones, *The CIA and American Democracy,* 2nd ed. (New Haven, CT: Yale University Press, 1989); Victor Marchetti and John D. Marks, *The CIA and the Cult of Intelligence* (New York: Dell, 1989); Lyman B. Kirkpatrick Jr., *The U.S. Intelligence Community: Foreign Policy and Domestic Activities* (New York: Hill and Wang, 1973); Admiral Stansfield Turner, *Secrecy and Democracy: The CIA in Transition* (Boston: Houghton Mifflin, 1985); *New York Times*, *The Tower Commission Report* (Toronto: Bantam Books, 1987); Bob Woodward, *Veil: The Secret Wars of the CIA 1981–1987* (Toronto: Pocket Books, 1987); Rhodri

Jeffrey-Jones, *Cloak and Dollar: A History of American Secret Intelligence* (New Haven, CT: Yale University Press, 2002); and U.S. Senate, *Foreign and Military Intelligence: Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities* (Washington: Government Printing Office, 1976). For the best examinations of similar Soviet activities, see Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story* (London: Hodder & Stoughton, 1990); Jeffrey T. Richelson, *Sword and Shield: Soviet Intelligence and Security Apparatus* (Cambridge, MA: Ballinger, 1986); John O. Koehler, *Stasi: The Untold Story of the East German Secret Police* (Boulder: Westview Press, 1999); Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive—The KGB in Europe and the West* (vol. 1) (London: Allen Lane, 1999), and *The Mitrokhin Archive—The KGB and the World* (vol. 2) (London: Allen Lane, 2005); Peter Deriabin and T. H. Bagley, *KGB: Masters of the Soviet Union* (New York: Hippocrene Books, 1990); John Barron, *KGB Today: The Hidden Hand* (New York: Reader's Digest Press, 1983); and Iain Phelps-Fetherston, *Soviet International Front Organizations* (New York: Praeger, 1965). For examinations of covert activities and operations otherwise, see Peter Grose, *Operation Rollback: America's Secret War Behind the Iron Curtain* (Boston: Houghton Mifflin, 2001); Jeffrey T. Richelson, *A Century of Spies: Intelligence in the Twentieth Century* (Oxford: Oxford University Press, 1995); Edward J. Epstein, *Deception: The Invisible War Between the KGB and the CIA* (Toronto: Simon & Schuster, 1989); Leslie Cockburn, *Out of Control* (New York: Atlantic Monthly Press, 1987); Gordon A. Craig and Alexander L. George, *Force and Statecraft: Diplomatic Problems of Our Time* (Oxford: Oxford University Press, 1983); Allen Dulles, *The Craft of Intelligence* (Toronto: Signet Books, 1965); Chapman Pincher, *The Secret Offensive—Active Measures: A Saga of Deception, Disinformation, Subversion, Terrorism, Sabotage and Assassination* (London: Sidgwick & Jackson, 1985); and Michael I. Handel, *War, Strategy and Intelligence* (London: Frank Cass, 1989). For studies dealing with other national intelligence and covert action activities, see (on the U.K.) Christopher Andrew, *Secret Service: The Making of the British Intelligence Community* (London: Heinemann, 1985), and Stephen Dorrill, *MI6: Fifty Years of Special Operations* (London: Fourth Estate, 2000); (on Israel) Claire Hoy and Victor Ostrovsky, *By Way of Deception: A Devastating Insider's Portrait of the Mossad* (Toronto: Stoddart, 1990), Dan Raviv and Yossi Melman, *Every Spy a Prince: The Complete History of Israel's Intelligence Community* (London: Houghton Mifflin, 1990), and Gordon Thomas, *Gideon's Spies: Mossad's Secret Warriors* (London: Macmillan, 1999); (on World War II) Michael Howard, *Strategic Deception in the Second World War* (London: Pimlico, 1990); and (on Chinese operations) Nicholas Eftimiades, *Chinese Intelligence Operations* (Annapolis: Naval Institute Press, 1990). For an assessment of covert action and intelligence since the end of the Cold War—and, in some cases, since the 2001 declared war on terrorism—see Loch K. Johnson, *Bombs, Bugs, Drugs and Thugs: Intelligence and America's Quest for Security* (New York: New York University Press, 2000); Loch K. Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (New Haven, CT: Yale University Press, 1996); John MacGaffen, "Clandestine Human Intelligence: Spies, Counterspies and Covert Action," and Henry A. Crumpton, "Intelligence and War: Afghanistan, 2001–2002," both in Jennifer E. Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington: Georgetown University Press, 2005); Len Scott, "Secret Intelligence, Covert Action and Clandestine Diplomacy," in Len V. Scott and Peter Jackson, eds., *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows* (London: Routledge, 2004); Roy Godson, *Dirty Tricks or Trump*

Cards: US Covert Action and Counterintelligence (London: Transaction, 2001); and Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington: Congressional Quarterly Press, 2000).

2. Johnson, *America's Secret Power*, p. 17.

3. Godson, *Intelligence Requirements for the 1980s*, p. 1.

4. Lowenthal, *Intelligence*, p. 106.

5. Johnson, *America's Secret Power*, pp. 16–17; Executive Order 12333 (1981) (3.4h, also 1.4d/f, 1.8e/f/i).

6. Johnson, *America's Secret Power*, p. 21. Bissell further breaks these down to (1) political advice, (2) subsidies to an individual, (3) financial support and technical assistance to political parties, (4) support of private organizations, (5) covert propaganda, (6) private training, (7) economic operations, and (8) paramilitary operations. Marchetti and Marks, *The CIA and the Cult of Intelligence*, p. 38.

7. Godson, *Dirty Tricks or Trump Cards*, p. xxxi.

8. James E. Steiner, "Restoring the Red Line Between Intelligence and Policy on Covert Action," *International Journal of Intelligence and Counterintelligence* 19, no.1 (Spring 2006), pp. 157, 158.

9. Blackstock, *The Strategy of Subversion*, pp. 78–94.

10. The term *guerrilla* originates with the period of Napoleon's occupation of Spain during the early nineteenth century when Spanish "guerrillas" (from the Spanish term *guerra*—"war"—with the *-illa* ending diminutive, meaning "little war") carried out a harassment, sabotage, and assassination campaign from their mountain hideouts against imperial French forces across Portugal and Spain. Lawrence's desert campaign evinced the exact same activities against the Turkish forces, using the desert (instead of mountains) as their hideout from which to engage in irregular (i.e., not regular) warfare—the epitome of covert paramilitary action witnessed during the Cold War.

11. Andrew and Gordievsky, *KGB: The Inside Story*, pp. 71–78.

12. The Irish Republican Army, formed of the Irish Republican Brotherhood and Irish Volunteers following the 1916 Easter Rising, formed the basis for the new National Army of the Irish Republic following its independence in 1922; this should not be confused with any of the organizations that have used that name since 1922.

13. For more on this, see Howard, *Strategic Deception*.

14. Andrew and Gordievsky, *KGB: The Inside Story*, p. 111.

15. Johnson, *America's Secret Power*, p. 19.

16. Maurer et al., eds., *Intelligence: Policy and Process*, p. 331.

17. As an example, sect.1.8(e) of Executive Order 12333 states that one of the roles of the CIA is to "conduct special activities approved by the President." *Special activities* is defined as "activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the [USG] is not apparent or acknowledged publicly" (3.4(h)-EO12333). Further authorization is given in sect.1.8(i): "conduct such administrative and *technical support activities* within and outside the United States as are necessary to perform the functions described . . . above, including procurement and essential cover and proprietary arrangements" (emphasis added). In this single phrase, Reagan justified the whole arms-for-hostages deal with Iran.

18. Johnson, *America's Secret Power*, p. 13.

19. X (Anonymous), "Sources of Soviet Conduct," *Foreign Affairs* 25, no. 4 (July 1947), pp. 575–76.

20. Johnson, *America's Secret Power*, p. 10.

21. Ibid., p. 14; Central Intelligence Agency, *Factbook on Intelligence* (Washington: CIA Public Affairs Office, 1990), p. 4.

22. Johnson, *America's Secret Power*, pp. 16–17; CIA, *Factbook*, p. 7.

23. U.S. Senate, *Foreign and Military Intelligence: Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities* (Washington: Government Printing Office, 1976), p. 475.

24. Kolko, *Confronting the Developing World*, p. 51; Ray S. Cline, *Secrets, Spies and Scholars: Blueprint of the Essential CIA* (Washington: Acropolis Books, 1976): 103; Richard Bissell states that the merging of the OPC with the CAS led to a blurring of the lines between the two functions of the CIA and eventual domination of CA over the collection mission (Marchetti and Marks, *The CIA and the Cult of Intelligence*, p. 329).

25. U.S. Senate, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, Book 1: *Foreign and Military Intelligence*, p. 145; Book 4: *Supplementary Detailed Staff Reports on Foreign and Military Intelligence*, p. 29.

26. Prados, *Presidents' Secret Wars*, pp. 29, 112–13.

27. Ibid., pp. 28–29.

28. Philip Agee, "Where Do We Go From Here?" in *Dirty Work: The CIA in Western Europe,* eds. Philip Agee and Louis Wolf (Secaucus: Lyle Stuart, 1978), p. 260.

29. Marchetti and Marks, *The CIA and the Cult of Intelligence*, p. 40.

30. Kolko, *Confronting the Developing World*, p. 5.

31. Prados, *Presidents' Secret Wars*, p. 468.

32. Marchetti and Marks, *The CIA and the Cult of Intelligence*, pp. 330–31.

33. U.S. Senate, *Final Report of the Select Committee*, Book 4, p. 68.

34. Ibid., p. 51.

35. Johnson, *America's Secret Power*, pp. 9, 18.

36. Congress attempted repeatedly to bring the intelligence community under legislative control because they feared it was becoming a unilateral security mechanism of the executive. For an in-depth account of this time, see Johnson, *A Season of Inquiry*, or Smist, *Congress Oversees*, as well as Cockburn, *Out of Control*.

37. Deriabin and Bagley, *KGB*, p. 383.

38. Andrew and Gordievsky, *KGB: The Inside Story*, p. 302.

39. Deriabin and Bagley, *KGB*, p. 387.

40. Epstein, *Deception*, p. 78.

41. Andrew and Gordievky, *KGB: The Inside Story*, pp. 57–58, 420, 384–85.

42. William R. Corson and Robert T. Crowley, *The New KGB: Engine of Soviet Power* (New York: William Morrow, 1985), p. 278.

43. W. E. Daugherty and Morris Janowitz, *A Psychological Warfare Casebook* (Baltimore, MD: Johns Hopkins University Press, 1956), p. 2.

44. Johnson, *America's Secret Power*, p. 22.

45. Quoted in Blackstock, *The Strategy of Subversion*, pp. 78–94.

46. Blackstock (*The Strategy of Subversion*) quoting Robert T. Holt and Robert W. van de Velde, *Strategic Psychological Operations and American Foreign Policy* (Chicago: University of Chicago Press, 1960), especially chaps. 1 and 2, pp. 1–54.

47. Blackstock (*The Strategy of Subversion*) quoting Julian Towster, *Political Power in the USSR, 1917–1947* (New York: Oxford University Press, 1948), p. 20.

48. For a discussion of the CIA's use of the media, see the Church Committee, *Final Report* (Washington, DC: U.S. Government Printing Office, 1976), Book 1, p. 192 specifically and pp. 191–201 generally; Johnson, *America's Secret Power*, p. 186.

49. Corson and Crowley, *The New KGB*, p. 379.

50. Pincher, *The Secret Offensive*, p. 1.

51. Prados, *Presidents' Secret Wars*, p. 123; Johnson, *America's Secret Power*, p. 23.

52. Cline, *Secrets, Spies and Scholars*, p. 128.

53. Treverton, *Covert Action*, p. 15.

54. Prados, *Presidents' Secret Wars*, p. 377.

55. Marchetti and Marks, *The CIA and the Cult of Intelligence*, p. 119.

56. Andrew and Gordievsky, *KGB: The Inside Story*, p. 419.

57. Ibid., p. 491.

58. Ibid., p. 406.

59. Ibid., pp. 418, 527.

60. Ibid., pp. 346, 495; Barron, *KGB Today*, p. 277.

61. Barron, *KGB Today*, p. 261.

62. Johnson, *America's Secret Power*, p. 184.

63. Declassified CIA Document DD1984-000091, Scott Library, York University (Toronto).

64. Johnson, *America's Secret Power*, p. 22.

65. Declassified CIA Document DD1984-000083, 1980-9C, Scott Library, York University (Toronto).

66. Johnson, *America's Secret Power*, p. 185; Church Committee *Report*, Book 1, p. 192.

67. Johnson, *America's Secret Power*, p. 186.

68. Treverton, *Covert Action*, pp. 14–15, 19.

69. Johnson, *America's Secret Power*, p. 197.

70. Treverton, *Covert Action*, p. 13.

71. Blackstock, *The Strategy of Subversion*, pp. 43–44, 56.

72. Quoted in Blackstock (*The Strategy of Subversion*): Harry Howe Ransom, *Can American Democracy Survive Cold War?* (New York: Doubleday, 1963), p. 176n.9.

73. Johnson, *America's Secret Power*, p. 25.

74. Ibid., pp. 25–26; Treverton, *Covert Action*, p. 20.

75. Johnson, *America's Secret Power*, p. 102.

76. Victor Marchetti and Panorama, "The CIA in Italy: An Interview with Victor Marchetti," in *Dirty Work: The CIA in Western Europe,* eds. Philip Agee and Louis Wolf (Secaucus: Lyle Stuart, 1978), p. 170; Agee, "Where Do We Go from Here?" p. 267.

77. Treverton, *Covert Action*, pp. 211–12.

78. Philip Agee and *Information Dienst*, "West Germany: An Interview with Philip Agee," in *Dirty Work: The CIA in Western Europe,* eds. Philip Agee and Louis Wolf (Secaucus: Lyle Stuart, 1978), pp. 185–86.

79. Philip Agee, "The CIA in Portugal," in *Dirty Work: The CIA in Western Europe,* Philip Agee and Louis Wolf (Secaucus: Lyle Stuart, 1978), pp. 67–68.

80. Edward Van der Rhoer, *The Shadow Network* (New York: Charles Scribner's Sons, 1983), pp. 6–8.

81. Andrew and Gordievsky, *KGB: The Inside Story*, p. 334.

82. See, for example, Christopher Andrew and Oleg Gordievsky, eds., *More "Instructions from the Centre": Top Secret Files on KGB Global Operations 1975–1985* (London: Frank Cass, 1992), pp. 29–31.

83. Pincher, *The Secret Offensive*, pp. 2–3, 7–12.

84. Prados, *Presidents' Secret Wars*, pp. 469–70.

85. Treverton, *Covert Action*, p. 20; Kolko, *Confronting the Developing World*, p. 217.

86. Johnson, *America's Secret Power*, pp. 22–23.

87. Kolko, *Confronting the Developing World*, p. 242.

88. Andrew and Gordievsky, *KGB: The Inside Story*, pp. 480, 413.

89. Ibid., pp. 466–68.

90. Prados, *Presidents' Secret Wars*, pp. 469–70.

91. Treverton, *Covert Action*, p. 21.

92. Epstein, *Deception*, p. 26; Corson and Crowley, *The New KGB*, p. 278.

93. Phelps-Fetherston, *Soviet International Front Organizations*, pp. 1, 2.

94. Most CIA corporate fronts were incorporated in Delaware due to its more lenient regulations regarding corporations (Marchetti and Marks, *The CIA and the Cult of Intelligence*, p. 118). For a full discussion of the CIA's use of proprietaries, see Church Committee *Report,* Book 1, pp. 205–56.

95. For a complete discussion of CAT, see Marchetti and Marks, *The CIA and the Cult of Intelligence*, pp. 121–24.

96. Prados, *Presidents' Secret Wars*, pp. 114–15, 116; Kirkpatrick, *The U.S. Intelligence Community*, p. 119n; for a complete discussion of Air America, as well as subsidiaries like Air Asia and Southern Air Transport, see Marchetti and Marks, *The CIA and the Cult of Intelligence*, pp. 124–26.

97. Marchetti and Marks, *The CIA and the Cult of Intelligence*, p. 120.

98. Ibid., pp. 408, 431–32, 375.

99. Prados, *Presidents' Secret Wars*, p. 450.

100. John Marks, "The CIA's Corporate Shell Game," in *Dirty Work: The CIA in Western Europe,* eds. Philip Agee and Louis Wolf (Secaucus: Lyle Stuart, 1978), pp. 127, 130.

101. Treverton, *Covert Action*, pp. 102–5.

102. Marks, "The CIA's Corporate Shell Game," p. 137; Prados, *Presidents' Secret Wars*, pp. 195, 211.

103. Arcos was funded through Amtorg (New York) and Wostwag (Hamburg), two fronts for the Comintern, and supported by the Cheka. It was later expelled from the United Kingdom for subversion, sabotage, political intrigue, and so on (Corson and Crowley, *The New KGB*, p. 283; Andrew and Gordievsky, *KGB: The Inside Story*, pp. 82, 84).

104. For more on the apartheid government's covert activities—both foreign and domestic—see Kevin A. O'Brien, "Counter-Intelligence for Counter-Revolutionary Warfare: The South African Police Security Branch," *Intelligence and National Security* 16, no. 3 (Autumn 2001), pp. 27–59; Kevin A. O'Brien, "Special Forces for Counter-Revolutionary Warfare: The South African Case," *Small Wars and Insurgencies* 12, no. 2 (Summer 2001), pp. 79–109; Kevin A. O'Brien, "The Use of Assassination as a Tool of State Policy: South Africa's Counter-Revolutionary Strategy 1979–1992 (Part II)," *Terrorism and Political Violence* 13, no. 2 (Spring 2001), pp. 107–42; and Kevin A.

O'Brien, "The Use of Assassination as a Tool of State Policy: South Africa's Counter-Revolutionary Strategy 1979–1992 (Part I)," *Terrorism and Political Violence* 10, no. 3 (Summer 1998), pp. 34–51.

105. Kirkpatrick, *The U.S. Intelligence Community*, p. 153; Church Committee *Report,* Book 1, p. 184; Marchetti and Marks, *The CIA and the Cult of Intelligence*, p. 41; Richard Fletcher, "How CIA Money Took the Teeth Out of British Socialism," in *Dirty Work: The CIA in Western Europe,* eds. Philip Agee and Louis Wolf (Secaucus: Lyle Stuart, 1978), p. 198.

106. Weissman et al., "The CIA Backs the Common Market," in *Dirty Work: The CIA in Western Europe,* eds. Philip Agee and Louis Wolf (Secaucus: Lyle Stuart, 1978), pp. 202, 203.

107. Johnson, *America's Secret Power*, p. 26; Treverton, *Covert Action*, p. 19.

108. Phelps-Fetherston, *Soviet International Front Organizations*, p. 1.

109. Andrew and Gordievsky, *KGB: The Inside Story*, pp. 57–58.

110. Phelps-Fetherston, *Soviet International Front Organizations*, pp. 3–4.

111. Richard Deacon, *A History of the Russian Secret Service* (London: Frederick Muller, 1972), p. 513; Barron, *KGB Today*, pp. 264–65.

112. Andrew and Gordievsky,*KGB: The Inside Story*, pp. 359, 419.

113. Ibid., pp. 419–20.

114. Ibid., pp. 492, 490, 506.

115. Johnson, *America's Secret Power*, p. 26.

116. *Counterintelligence* is defined as "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities" (Executive Order 12333, 3.4a)

117. Charters, "The Role of Intelligence Services," p. 334.

118. Keylor, 221; Cockburn, *Out of Control*.

119. Johnson, *America's Secret Power*, pp. 12–13.

120. Ibid., p. 26.

121. Ibid., pp. 26–27.

122. Ibid., pp. 28–29.

123. Begun in 1952, USAID sent public safety missions to over thirty-eight nations between 1955 and 1962; by 1973, over 73,000 foreign police personnel had been trained. That year, however, Congress banned USAID from continuing such operations, and the project was taken over covertly by the CIA: Johnson, *America's Secret Power*, p. 157, this was exposed in a 1966 issue of *Ramparts*; Kirkpatrick, *The U.S. Intelligence Community*, p. 151; Kolko, *Confronting the Developing World*, pp. 50–51, 131, 210.

124. Church Committee *Report*, p. 269.

125. Prados, *Presidents' Secret Wars*, pp. 40–41, 55–58, 120–21.

126. Ibid., pp. 269–94, 271, 291.

127. Deriabin and Bagley, *KGB*, p. 388.

128. Epstein, *Deception*, pp. 282, 283–90.

129. Deriabin and Bagley, *KGB*, p. 363.

130. Andrew and Gordievsky, *KGB: The Inside Story*, p. 384; Van der Rhoer, *The Shadow Network* 11–12.

131. Deriabin and Bagley, *KGB*, pp. 358–59.

132. Blackstock *The Strategy of Subversion*.

133. Blackstock (*The Strategy of Subversion*) quoting a "former high-ranking Israeli intelligence officer and confirmed by Allen Dulles during a public visit, as a guest lecturer, to the University of South Carolina, April 2, 1963."

134. Bob Woodward, *Bush at War* (New York: Simon & Shuster, 2002), p. 78.

135. For a good summary of this, see Susan Wright, "The Hijacking of UNSCOM," *Bulletin of the Atomic Scientists* 55, no. 3 (May/June 1999), pp. 23–25.

136. Prados, *Presidents' Secret Wars*, p. 466.

137. Treverton, *Covert Action*, p. 22.

138. Kolko, *Confronting the Developing World*, p. 105.

139. Prados, *Presidents' Secret Wars*, pp. 465–66.

140. Johnson, *America's Secret Power*, p. 69.

141. Ibid., p. 196.

142. Ibid., p. 84; Prados, *Presidents' Secret Wars*, p. 383.

143. Prados, *Presidents' Secret Wars*, pp. 469–70, 125.

144. Epstein, *Deception*, p. 41.

145. Andrew and Gordievsky, *KGB: The Inside Story*, pp. 420, 528.

146. Ibid., p. 494.

147. Deriabin and Bagley, *KGB*, p. 364.

148. Prados, *Presidents' Secret Wars*, p. 467.

149. Treverton, *Covert Action*, p. 3.

150. John Le Carré, *The Secret Pilgrim* (Toronto: Viking, 1990), pp. 334–35.

3

COVERT ACTION

The Israeli Experience

EPHRAIM KAHANA

COVERT ACTION HAS ALWAYS BEEN A SIGNIFICANT element of international politics. When it has served their interests, governments have secretly disseminated propaganda in other countries, manipulated foreign economies, and abetted coups against their adversaries, on either a direct or indirect basis.

Israel, like other countries, has and uses the tool of covert action, with varying degrees of success. Israeli covert action includes the full range of options, inclusive but not limited to paramilitary incursions and the rescue of Jews from foreign territories. In this chapter, the most significant and sometimes most controversial covert actions are described.

THE BAD BUSINESS

The Bad Business, known in Hebrew as the *Esek Ha'Bish*, was the most controversial Israeli covert action to date in the public domain. This covert action is commonly known as well as either Operation Susannah, or the Lavon Affair, named after the Israeli Defense minister of the period (1954), Pinhas Lavon. In essence, the Bad Business was a paramilitary action of sabotage against primarily American/British targets in Egypt.[1]

Egypt, historically the largest and most powerful of Israel's neighboring Arab countries, was always of primary interest to the Israeli intelligence services. At Military Intelligence (MI), it was decided to set up a network of sleeper agents in Egypt, who, at the appropriate time, would be assigned to carry out secret missions. In May 1951, an Israeli intelligence officer from Unit 131, Maj. Avraham Dar, was secretly dispatched to Egypt under the assumed name of John Darling,

using the cover of a British businessman, with a mission to recruit Egyptian Jews for an espionage network. Dar succeeded in this task fairly easily, because several young Egyptian Jews with Zionistic tendencies simply volunteered. Dar set up two espionage cells, one in the port city of Alexandria and the other in Cairo. With respect to the Cairo cell, Dar recruited Ceasar Cohen, Moshe Marzouk, Eli Ya'acov Naim, and Victorine Marcel Ninio as operatives. For the Alexandria cell, he recruited Shmuel Becor Azzar, Robert Nissim Dassa, Victor Moise Levy, Meir Shmuel Meyuhas, Philip Hermann Nathanson, and Meir Yosef Za'afran. Several of the candidate agents were transported secretly to Israel for military training and tradecraft. Despite the fact that many remained rank amateurs after the training, the operatives were nonetheless sent back to Egypt. They "slept" for three years until the agreed code word was broadcast over the army radio channel, *Galei Zahal.*

Toward the end of 1951, Avraham (Avri) Elad, a former major in the Israeli Defense Force (IDF), contacted Dar and the commander of Unit 131, Lt. Col. Mordechai (Motke) Ben-Tsur, to seek employment. Despite certain reservations, the heads of Unit 131 decided to involve Elad in the operation, and he was assigned cover as a German businessman named Paul Frank. Elad resided initially in West Germany to construct and develop his cover story further. In December 1953, Elad arrived in Egypt (as Paul Frank), a wealthy businessman. He soon blended into the expanding colony of expatriate Germans, many of whom were past Nazis. Elad was to take command of the sleeping Jewish espionage network. He contacted all its members and became closely acquainted with their details.

After the revolution in Egypt in 1952, the United States exerted pressure on Britain to withdraw from the Suez Canal zone to keep Egypt in the pro-Western camp. There was concern in Israel concerning the forthcoming British evacuation because the Israeli government regarded the presence of British forces in the canal zone as a check and balance against possible Egyptian adventurism under Gamal Abdel Nasser. However, by the end of June 1954, the British evacuation of the Suez Canal zone appeared imminent. Israeli Defense Minister Lavon asked Binyamin Gibli, the director of MI, to use all of Unit 131's resources in Egypt to prevent the British pullout. Lavon, however, did not immerse himself in the details of strategy, to his discredit. Accordingly, Gibli came up with the idea of preventing or delaying the British withdrawal by staging a series of sabotage acts directed primarily against Western embassies and other institutions that would, according to Gibli, be interpreted by the British as acts being perpetrated by the Egyptians. Gibli believed that under such circumstances the British might reconsider the planned evacuation program.

On June 30, 1954, Gibli instructed Elad to carry out the covert sabotage in Egypt, resulting in small firebombs being placed in mailboxes in Alexandria two days later. On July 14, small, harmless bombs exploded at the U.S. cultural centers in Cairo and the library of the U.S. Information Center in Alexandria, as well as in the luggage storage depot at the Alexandria Railway Station.

However, when Philip Nathanson entered the Rio Cinema in Alexandria, the charge he was carrying went off prematurely, which resulted in his arrest. Within days the Egyptian security police arrested and interrogated the rest of the network's members. They also arrested Max Binnet, another Israeli spy working under cover at the time in Egypt, but who was not directly connected to the group.

Members of the MI's inner circle were forced to accept responsibility for recruiting and training Egyptian Jews for their espionage network, while Gibli admitted the operatives clandestine duties—however, these admissions were not made public. Prime Minister Moshe Sharett knew nothing of the operation. Gibli asserted that the order to activate the operatives was given to him by Lavon.

After the capture of the espionage network's members in Egypt, Gibli tried to activate a European lobby to ease the Egyptians' treatment of their Israeli-trained Jewish prisoners, who were being interrogated under torture in appalling conditions in an Egyptian jail. A trial began on December 11, 1954, with the sentencing a month later. Cohen and Na'im were acquitted. Meyuhas and Za'afran were each sentenced to seven years, and Ninio and Dassa each received fifteen years in prison. Levy and Nathanson were sentenced to life imprisonment, whereas Azzar and Marzuq were sentenced to death and executed. Dar and Elad, the Israeli handlers of the network, were tried in absentia and sentenced to death. Max Binnet, the Israeli spy apprehended with the network but not directly involved in its operations, committed suicide in an Egyptian jail on December 21, 1954, after undergoing severe torture sessions.

For years, Israel denied any connection to the bombing in Egypt, with the local media being barred by the military censor from mentioning the affair. Since the story was published in the foreign press, Israeli inner circles began to demand the establishment of a commission of inquiry. Subsequently, Israeli weekly publication *Ha'Olam Ha'Zeh* printed the story without the censor's permission with an invented name for the country involved.

Ultimately the scandal was made public, and Lavon was forced to resign. David Ben-Gurion returned from retirement and replaced Lavon as Minister of Defense. In 1960, new evidence emerged from a secret trial of Elad, held in 1958. Apparently it is understood that Elad betrayed the Jewish network in Egypt. The Israeli establishment remained anxious, fearing the opening of a Pandora's box regarding the person who gave the order to activate the Jewish network in Egypt. Subsequently, Lavon asked Ben-Gurion to exonerate him, but Ben-Gurion refused.

Several Israeli commissions investigated the Bad Business, but they failed to reach unambiguous conclusions as to who gave the order or who was responsible for the fiasco. In 1960, a commission revealed the forging of a document used by Moshe Dayan and Shimon Peres, then deputy minister of Defense, to attract the responsibility for the botched 1954 Egyptian operation to Lavon. In a subsequent hearing, the results of which were accepted by the government, it was revealed that Peres, Dayan, and Gibli were all involved.

The specific question of "who gave the order?" has been asked countless times by the Israeli public, yet it appears the answer will not be forthcoming. A more important question revolves around who was responsible for the Bad Business, even if it was not that person who actually gave the order. The answer to this question is definitive; as the supreme commander of the IDF, the Israeli government bears the ultimate responsibility for all military intelligence failures, including this one. This also applies to the minister of Defense, even if he did not give the specific order.

In the aftermath of the Sinai Campaign in October 1956, it seemed reasonable to expect negotiations for the release of the prisoners of the Jewish espionage network. Israel held over 5,500 Egyptian POWs after its conquest of the Sinai Peninsula. Among the most senior of the captives was Gen. Fuad el Digwi, who had been the presiding judge at the trial of the members of the Jewish espionage ring in 1954. When he fell into Israeli custody, he was the military governor of the Gaza Strip. All 5,500 Egyptian prisoners were consequently traded for 10 Israeli POWs, including one pilot. The Israeli government did not request the release of the members of the Jewish network from prison because its policy was still to deny any Israeli connection to the events in Egypt in 1954. Top Israeli echelons believed that requesting the prisoners release might endanger Israel's relations with the United States.

After fourteen years of rotting in Egyptian jails, Dassa, Levy, Nathanson, and Ninio were released, as part of the agreement to return 5,237 Egyptian POWs captured during the 1967 Six-Day War. The four members of the network were released separately from the Israeli POWs and reached Israel via Europe. This time the inclusion of the Jewish spy network prisoners in the POW exchange was settled only at the insistence of the director of the Mossad, Meir Amit, who threatened to resign if he would not be allowed to seek their release during negotiations with the Egyptians. For all that, the presence in Israel of the released network members remained an official secret until Prime Minister Golda Meir announced her intention to attend Marcelle Ninio's wedding in 1971 and to inform the Israeli press.

The key result of the Bad Business was that the Israeli government adopted a tenet of never activating Jews in the diaspora for espionage or any other covert action against their own country's government, with a belief that such activity might ruin relations between the Jewish citizens of such countries and their government. In nondemocracies, like the Arab states, activating Jewish spies would in any case have a limited effect, because their access to important governmental positions or secrets, if any, is negligible. The Pollard Affair by definition is dissimilar in nature. Jonathan Jay Pollard was not operated by an official intelligence organization in Israel but by an amateur outfit known as the Bureau of Scientific Liaison, known by its Hebrew acronym as LAKAM.

On March 30, 2005, the three last surviving members of the espionage network in Egypt, Ninio, Dassa, and Za'afran, were accorded recognition by Israel's President Katsav and the chief of the General Staff Lt. Gen. Moshe

Ya'alon, for their services to the state and their years of incarceration and suffering.[2]

THE KHALED MASHAL FIASCO

The Khaled Mashal fiasco occurred on September 24, 1997, when members of the Kidon (bayonet) Unit of the Mossad arrived in Jordan, where they checked in as tourists at the Intercontinental Hotel in Amman. Two of them, who used fake Canadian passports in the names of Barry Beads and Sean Kendall, were to execute the team's mission, which was to assassinate Khaled Mashal, the leader of Hamas, whom Israel believed to be behind many terrorist attacks that cost the lives of Israeli civilians. The Israeli Committee X, chaired by Prime Minister Benjamin Netanyahu, had decided on the assassination, determining that the mission should be accomplished on Jordanian soil. Although Mashal resided in Jordan, this was a curious decision at best, considering the extremely delicate Israeli-Jordanian relations after the two countries signed a peace treaty in 1994.[3]

The day after their arrival, "Beads" and "Kendall" attempted to poison Mashal in a crowded Amman street by spraying him with a nerve agent. They barely managed to use only half the aerosol can's content when their actions were observed, and they fled the scene immediately but were later arrested. Mashal was hospitalized, while the support members of the Kidon Unit succeeded in departing Jordan.

This fiasco caused enormous embarrassment to both governments and jeopardized Israel's relations with one of its few Middle Eastern allies. King Hussein threatened Netanyahu that he would put the men on trial if the Mossad did not provide an antidote to save Mashal's life. Israel acceded to Hussein's demand and Mashal was saved.

At the demand of Hussein, Israel also released Hamas leader Sheikh Ahmed Yassin, imprisoned in Israel for his role in terrorist acts. The two Mossad agents were delivered to the Canadian embassy in Amman and driven to Israel, with the Israeli government assuring the Canadians that it would never again use false Canadian documents. The Khaled Mashal fiasco was considered the second Bad Business; however, the period was different and this fiasco almost immediately became public, unlike the Bad Business.[4]

OPERATION WRATH OF GOD

The Munich massacre of the Israeli athletes during the 1972 Olympic Games shook the Israeli defense establishment to its very foundations, and the street demanded vengeance. Golda Meir's government was indeed bent on revenge, and its first response was a massive air bombardment of terror bases in Lebanon. Three days later, the Israel Air Force launched an air raid involving approximately

seventy-five aircraft, the largest such attack since the 1967 Six-Day War. Israeli ground troops were additionally ordered into Lebanon to engage Palestinian terrorists who had been mining Israeli roads. Despite this aggressive military response, a select group of high-ranking Israeli officials felt that more had to be done. They decided that a message should be sent not only to those who had perpetrated the Munich massacre but also to those who might consider terrorist attacks against Israelis in the future, so that others might see and fear.[5]

This led to the decision to establish the so-called Committee X, chaired by Meir and Defense Minister Moshe Dayan. The committee authorized the assassination of all the individuals involved, either directly or indirectly, in the Munich massacre. Committee X listed thirty-five main assassination targets. The mission was assigned to several different Mossad teams, formed by the commander of the Caesarea Division in the Mossad, Michael (Mike) Harari. It was carried out mainly by Kidon (bayonet), an ultra-secret subunit of Caesarea.

The operations conducted to assassinate key Palestinian terrorist leaders were known by their unofficial names: Operation Wrath of God and the Sword of Gideon. A general mobilization was declared within the Israeli Security Agency (ISA) and in Unit 504 of the IDF. For the purpose of the assassinations, the most talented intelligence-gathering officers were called up, including Shmuel Goren, commander of Keshet (an intelligence-gathering unit), Baruch Cohen, Zadok Ofir, Raphael (Rafi) Sutton, Eliezer (Geyzi) Tsafrir, and Nahum Admoni, commander of Tevel, the branch in charge of connections with foreign intelligence agencies.

During the search for the terrorists involved in the Munich massacre, it emerged that of the eight who had taken part in the massacre, five had been killed by the German police officers and three had been detained. After the hijacking of a Lufthansa airliner in October 1972, the detained terrorists were released to Libya and then onto Damascus, whereupon traces of them were lost. As far as is known now, they were still alive. However, about twenty other Palestinians with blood on their hands or who had been involved in preparing acts of terror but were not necessarily connected to the Munich massacre met their deaths in strange and mysterious ways.

In any event, the Munich massacre signified a real turning point in Israel's war on terror. This was the beginning of a war to the death against the terror organizations, a campaign of elimination and vengeance. One of the first targeted for assassination, whose name and nickname are still classified, was a Black September Organization (BSO) member who arrived in Athens with the task of sending a container of raisins covering hidden explosives to the Haifa port, where it would be detonated by remote control.

The Mossad received information about this plan, and its operatives left for Athens, where they searched for the perpetrator. They discovered a female customs broker who, unknown to her, was handling that cargo of raisins bound for Israel. Documents were seized, and through them Mossad agents located the storage depot where they hoped to find the raisin bomb, but nothing was discovered. The

documents did reveal, however, the man behind the shipment, who was then followed and shot dead. BSO members concluded that the customs broker had given details about their comrade's activities to the Mossad, and they killed her.[6]

According to George Jonas's book *Vengeance*, one of the teams assigned to assassinate Palestinian terrorists was headed by a former IDF officer, who was referred to in his book by the pseudonym Avner, who controlled a team of five operatives and operated in a semi-autonomous fashion. It is, however, impossible to verify the existence of Avner and his specific team. As it is better known today, Kidon's teams were assigned to assassinate a list of targets, as follows: Kamal Adwan, the chief of sabotage operations for the Al Fatah organization in the 1967 occupied territories; Hussein Abad Al-Chir, the Palestinian Liberation Organization (PLO) contact man with the KGB in Cyprus; Mohammed Boudia, the BSO liaison with the European PLO; Abu Daoud, a BSO member; Dr. Wadi Haddad, a chief terrorist linked with Dr. George Habash; Mahmoud Hamshari, a PLO member and coordinator of the Munich Olympic Games massacre; Dr. Basil Raoud Kubaisi, an official of the Popular Front for the Liberation of Palestine (PFLP) in charge of logistics; Kamal Nasser, the official PLO spokesman and a member of the PLO Executive Committee; Ali Hassan Salameh, a developer and executor of the assault on the Israeli athletes at Munich; Abu Yussuf, a high-ranking PLO official; and Wael Zwaiter, a PLO organizer of terror in Europe and Yasser Arafat's cousin. Kidon's teams succeeded in tracking down and killing several of the targets on the list: Zwaiter on October 6, 1972; Hamshari on October 8, 1972; Abad al-Chir on January 24, 1973; Kubaisi on April 6, 1973; and Boudia on June 28, 1973. After killing Abad al-Chir, Ziad Muchassi replaced him as the PLO contact with the KGB, and he was belatedly added to the target list. He was killed on April 12, 1973.

As for the other targets listed by Committee X, six terrorists remained at large. Wadi Haddad was not traced by Israel, but he died of cancer on March 28, 1977 in an East Berlin hospital. Abu Daoud was arrested in Germany in March 1973 and confessed to his involvement in the Munich massacre. Kamal Adwan, Kamal Nasser, and Abu Yussuf were killed by a covert commando raid on April 9, 1973, carried out as a joint Mossad-IDF mission (see Operation Spring of Youth). Ali Hassan Salameh was killed on January 22, 1979, in a Beirut car bomb explosion by another Mossad team.

A high price for Operation Wrath of God was paid by Mossad personnel who collected intelligence data about those marked for elimination. For example, following an arranged meeting with a Palestinian in a café in Madrid, Baruch Cohen was shot dead by another Palestinian as he was leaving the café. Likewise, Zadok Ofir was gravely wounded in Brussels at his meeting with a dubious informer. Other members of the team that mistakenly killed Ahmad Bouchiki (in Lillehammer, Norway) were arrested in Oslo, and four members of the team, Dan Arbel, Marianne Gladnikoff, Sylvia Raphael, and Michael Dorf, were sentenced to prison terms.

OPERATION DAMOCLES

Operation Damocles was another paramilitary operation of assassination. After the 1956 Sinai Campaign, Egyptian President Gamal Abdel Nasser requested West Germany to build a surface-to-surface missile capability that could be used in future Egyptian wars against Israel. In 1962, Mossad Chief Isser Harel learned that work on the project had begun and requested Israeli Prime Minister David Ben-Gurion to seek the intervention of West German Chancellor Konrad Adenauer to halt it. Ben-Gurion however, was determined not to clash with the West German government. At his own initiative, Harel set in motion subversive actions with the overall title of Operation Damocles against German scientists and their families working on the project in Egypt. This campaign involved abductions and letter bombs, causing the deaths of at least five people between 1962 and 1963. Several letters were mailed by an Israeli spy in Egypt, Wolfgang Lotz. Aharon Moshel, another Israeli spy in Egypt, also engaged in hunting German scientists in that country.

Measures against Germans involved in the missile project were mainly under the command of Joseph (Joe) Ra'anan, who had joined the Mossad after serving as an intelligence officer in the Israel Air Force, and Yitzhak Shamir, who later became prime minister of Israel. One success was the disappearance of Dr. Heinz Krug, probably murdered in September 1962. In February 1963, Dr. Hans Kleinwachter, an electronics specialist, who in World War II was engaged in Nazi Germany's V2 rocket project, survived an assassination attempt by Shamir's team.

In the 1950s, Israel decided to clandestinely assassinate the chief the Egyptian commanders of the Palestinian terrorism. Col. Hafez Mustafa, then commander of Egyptian Intelligence in the Gaza Strip, was listed as a target and was assassinated. At that time, Egypt customarily sent cells of marauding Arabs (*Fedayeen*) from the Gaza Strip into Israel for the purpose of terrorizing Israeli society by murdering Israelis. Mustafa was in charge of those operations.

In June 1956, the director of Israel's DMI Maj. Gen. Yehoshafat Harkabi proposed a plan to assassinate Mustafa, which was successfully carried out on June 12, 1956, by an explosive device hidden in a book handed to him by an Egyptian double agent. Another book bomb was sent the following day via an East Jerusalem post office to Col. Salah Mustafa, Egypt's Amman-based military attaché, who had dispatched infiltrators via the West Bank into Israel. He opened the package and was killed by the blast. In the 1960s mail bombs became a central assassination tool of Israeli intelligence, especially against (former Nazi) German scientists who were involved in developing a missiles program for Egypt.

These paramilitary covert actions were not designed to be made public; their goals were to enhance Israeli security. The Bad Business and the Khaled Mashal affair became public knowledge because they failed. Operation Wrath of God was never officially connected to Israel, consequently Israel has never admitted partaking in the killings. However, Israeli fingerprints were well stamped on these operations. Two more covert actions of assassination in which Israel has

never admitted playing any part were the assassinations of Abu Jihad and Yahya Ayyash.[7]

The Engineer was the nickname of Ayyash, who was born in 1966 near Nablus and studied electrical engineering at Bir Zeit University near Ramallah, where he joined Hamas. During a 24-month campaign of terror beginning on April 6, 1994, Ayyash killed 130 Israelis and wounded nearly 500. As the carnage in the streets of Israeli cities grew, Ayyash became revered by masses of Palestinians. One of the largest manhunts in Israeli history was mounted for Israel's most wanted man, involving the British Secret Service (MI5), the Royal Jordanian Special Forces, the FBI, and the New York City Police Department. In charge of catching Ayash was the ISA. The ISA, among the elite of Israel's security agencies, succeeded in handing Ayyash a mobile phone via an operative. On January 5, 1996, the cell phone was detonated after Ayyash answered an incoming call, and he was killed. More than 100,000 Palestinians attended his funeral.[8]

THE SPRING OF YOUTH

Other paramilitary covert actions were carried out secretly but became public immediately after the operation ended. These operations were covert for tactical purposes only, to maintain the effect of surprise. Operation Spring of Youth was one of these, and it remained covert as long as the forces were engaged in the field. The operation was launched on April 9, 1973, and was carried out by approximately forty highly trained commandos of the most elite unit of the IDF, Sayeret Matkal. Its purpose was to avenge the deaths of the Israeli athletes slaughtered at the 1972 Munich Olympics by eliminating those in any way responsible for the massacre.[9]

In February 1973, Lt. Col. Ehud Barak, the commander of Sayeret Matkal, obtained photographs and precise information as to the whereabouts of three Palestinians involved in the massacre, Kamal Adwan, Kamal Nasser, and Mahmoud Yussuf Najjer, better known as Abu Yussuf, who were all then residing in Beirut. The Mossad obtained information that two of them lived on the second and third floors of the same building in Beirut, and the third lived across the street. The information also specified the exact architectural plans of the buildings.

After cross-referencing the intelligence, the strategy selected and executed by Sayeret Matkal was for the commando teams to infiltrate the Lebanese border by sea, disguised as tourists, with their weapons hidden. The distance from the beach landing point to the Beirut target apartments was approximately six miles. Three commando units would attack the individual apartments, and a guard unit would be positioned outside the apartment to contain any Lebanese police, army, or Palestinian reinforcements. The operation was calculated to last twenty minutes from the time of the initial shots until Lebanese or Palestinian reinforcements arrived on the scene. By then the commandos were expected to be back on the beach boarding the craft that would return them to Israel.

Barak, dressed as an Arab woman, commanded the operation and lead the guard unit. Another officer, Amiram Levine, was also disguised as an Arab woman. This unit maintained contact with their forward operational headquarters located aboard Israeli navy boats, offshore from Beirut.

Alighting on the Lebanese coast, the commandos were met by three cars driven by Mossad operatives, planted in Lebanon beforehand, who had intimate knowledge of the city. They drove the commandos to the apartments and returned them to the beach once the operation was accomplished. The drivers were Gilbert Rimbaud (Belgian) and Dieter Altnuder (German). In addition to the three apartments, a unit from the Israel Paratroop Regiment, led by Amnon Lipkin-Shahak, was assigned to strike the six-story headquarters of the world's most notorious hijacker, Dr. George Habash of the PFLP. Another paratrooper unit, as well as the Naval Commando Unit Sayetet 13, were to raid weapons manufacturing facilities and fuel dumps that the PLO maintained in the Tyre-Sidon area.

Among other well-known officers who took part in Operation Spring of Youth were Muki Betser and Yoni Netanyahu; the latter was killed in 1976 in Operation Yehonathan (also commonly known as Operation Entebbe).

Operation Spring of Youth succeeded because of excellent intelligence and ground assistance carried out by the Mossad. All the commandos of the Sayeret Matkal returned alive from the operation, with one wounded. During the (paratrooper) raid led by Lipkin-Shahak, two soldiers were killed.[10]

OPERATION YEHONATHAN

Operation Yehonathan was another covert operation carried out for tactical purposes of surprise: a rescue mission of Israelis who were hijacked by terrorists to Uganda. This operation, which took place on the night between July 3–4, 1976, came belatedly to be known as Operation Yehonathan, in honor of Lt. Col. Yehonathan "Yoni" Netanyahu, who was killed during the operation. The same operation was additionally known as Operation Entebbe, Operation Thunderball, or Operation Thunderbolt.[11]

On June 27, 1976, Air France flight 139 from Israel to Paris with 246 passengers was hijacked after taking off from its stopover point in Athens, Greece. It was diverted to Benghazi Airport in Libya, then onto Entebbe Airport in Uganda, where it landed. Eight of the hijackers were PLO members, and two belonged to the Baader-Meinhof gang. They were apparently supported by the Ugandan regime of pro-Palestinian President Idi Amin. In their ultimatum, the hijackers demanded that the government of Israel release all convicted Palestinian terrorist murderers; they set a 3-day deadline of June 30.

In principle the government of Israel is against any kind of negotiating or bargaining with hijackers, because to do so might serve as a precedent for further hijacking attempts. The alternative option, in this instance, was a rescue attempt by means of a military operation. The IDF chief of the General Staff, Lt. Gen.

Mordechai Gur, was reluctant to recommend a military rescue operation unless relevant and updated intelligence was gathered. The only information at hand concerned the blueprints of the terminal building at Entebbe Airport, obtained from the Israeli construction firm Solel Boneh, which had constructed the building in the 1960s. But this intelligence was insufficient. Parallel to the planning of a military rescue operation of the passengers, the Israeli government stated its readiness to pursue several political paths for the release of the hostages, which was a ploy to gain time for acquiring more intelligence on the situation and planning the rescue operation. As the negotiations proceeded, the hijackers extended their ultimatum to July 4.

The passengers were held in the old terminal's transit hall. The terrorists subsequently freed a large number of them, keeping only Israelis and Jews, whom they threatened to kill if the Israeli government did not meet their demands. The hijackers said they would free the airplane's crew, and an Air France plane was sent to Entebbe for that purpose. The plane's captain, Michael Bacos, and his crew refused to depart without all the passengers and accordingly remained with the hijacked passengers. One hundred three Israelis—men, women, and children—remained hostage in Entebbe.

Following the release of the non-Israeli/non-Jewish hostages, reserve Lt. Col. Amiram Levine in the Collection Department of the DMI flew to Paris on July 1 with Lt. Col. Amnon Biran to collect all possible information from the freed hostages, only two of whom remembered varying levels of detail.

At a preset time, four Hercules transport aircraft flew to Entebbe Airport and night-landed without any ground aid. They were followed by an Israeli air force jet with medical facilities that flew into Nairobi Airport in Kenya. Over 100 Israeli soldiers, including members of the elite Sayeret Matkal Unit, arrived to conduct the assault with Mossad operatives alledgedly taking part by way of providing ground assistance.

The aircraft landed an hour before midnight on July 3, 1976. A black Mercedes Benz limousine with an accompanying jeep convoy were driven toward the airport buildings to divert attention. It was hoped that this cavalcade would be taken to signify the arrival of a high Ugandan official with his escort, possibly Amin himself. Meanwhile the Israeli troops drove from the aircraft to the terminal building.

The raid took place during the early hours of July 4 and lasted about three minutes. Six or eight terrorists were killed, and all the hostages in the terminal were released alive, except for one who was killed when he frantically leaped at the Israeli forces. Another hostage, 75-year-old Dora Bloch, who was recovering from a choking episode in a Kampala hospital on the night of the raid, was left behind in Uganda and later murdered by two Ugandan army officers. During the incursion, Ugandan forces opened fire on Israeli troops, killing Netanyahu. Forty-five Ugandan soldiers were killed during the raid, and the Ugandan Airforce fighter planes parked on the ramp were taken out of action. Shortly after the fighting ceased, the rescued hostages were flown out via Nairobi to Israel.

One of the factors behind the excellent planning of the raid was superior intelligence. The success of Operation Yehonathan was result of the first-class troops of Sayeret Makal, but also, and no less importantly, to the essential information obtained by Israeli intelligence. The successful rescue from Entebbe Airport, a little less than three years after the failure to provide an early warning on the eve of the 1973 Yom Kippur War, afforded a major boost to morale among Israeli intelligence officers.[12]

COVERT RESCUE MISSIONS

Other covert actions were carried out for purposes of rescuing Jews from hostile Arab dictatorships. In 1970, intelligence began to trickle into the Israeli government from Syria with respect to privations suffered by the Jewish communities in Aleppo and Damascus. The reports told of young Jews making an effort to flee Syria, despite the difficulties and the dangers. The Israeli government, under Golda Meir, resolved to embark on an operation to bring the Syrian Jews to Israel. Operation Blanket began in 1970 and lasted several years; it was in fact a series of individualized and intricate operations. The operations were carried out by combat troops of Naval Commando Shayetet 13 of the Israeli navy, acting under orders of the Mossad, which was charged with the implementation of the operations. As part of the overall plan, Mossad operatives made dozens of incursions into Syria, as did combatants of Shayetet 13.

The Israeli government invested many resources in Operation Blanket, which in total succeeded in taking to Israel only a few dozen young Jews. The operational participants made the Syrian capital almost their home while taking enormous risks. Moreover, this was a mere few years after the capture and execution of an Israeli spy in Syria: Eli Cohen. Other covert actions for purposes of rescuing Jews that became well known were Operations Moses and Solomon. However the first rescue-type operations were Operations Magic Carpet and Tushia.

Operation Magic Carpet involved the secret airlifting of Yemeni Jews to Israel. Toward the end of April 1949, the imam of Yemen agreed to let most of the Jews, some 45,000 out of around 46,000, depart the country of their birth, Yemen. From remote corners of the country, the Yemeni Jews made their way on foot to an airport where they unobtrusively boarded Israeli transport aircraft, totaling 380 flights, to Israel. British and American airplanes were also engaged in the airlift. Most of these impoverished and isolated Jews had never seen an airplane, and on landing in Israel described their flying mode of transport as a "magic carpet." Thus Operation Magic Carpet became the name of this highly complex and dangerous rescue-immigration campaign. Operation Magic Carpet ran from May 1949 to the end of September 1950. Operatives of the Mossad Le'Aliyah Beth were dispatched to Yemen to organize the operation, which was kept secret and revealed to the media only after completion.[13]

Operation Tushia (meaning "initiative" in Hebrew) was carried out in 1956 after the Sinai Campaign. The operation was executed by Israeli intelligence in the hope that its operatives in Egypt would be in a position to contact Egyptian Jews and persuade most to leave for Israel. On November 9, 1956, Maj. Avraham Dar and Aryeh (Lova) Eliav, together with their radio operator, slipped into the war zone pretending to be French officers in French military uniforms and advanced with the British and the French troops. In Port Said they found only 200 mostly elderly Jews with no interest in moving to Israel. In the Jewish synagogue in the town they encountered only sixty-five Jews willing to leave with them for Israel. Secretly the three took them to the harbor and with the assistance of the French army, boarded them onto two French military landing craft. After sailing about one and a half miles offshore, the French craft met up with two tiny Israeli navy vessels camouflaged as Italian fishing boats, which carried the Egyptian Jews to Israel, with Dar and Eliav following days later.[14]

Operation Moses, known in Hebrew as Mivtza Moshe, came to fruition in 1974 after Ethiopian Emperor Haile Selassie was overthrown by a Marxist regime, resulting in the local Jewish community suffering in the Marxist revolutionary chaos. In 1977 and for several more years, Ethiopian Jews began arriving in Israel. As economic and political conditions in Ethiopia deteriorated, tens of thousands of Jews set out to cross the border into neighboring Sudan. In 1979, Israel (and to a lesser degree private organizations) began to evacuate the Ethiopian Jews from Sudan to Israel by various covert means. As word reached the Jewish villages in Ethiopia that the route to Israel was through Sudan, the flow of refugees across the border increased dramatically. The Mossad, through it Tsafririm Unit, was tasked with handling the rescue of the Ethiopian Jews. During winter 1984, it became clear that the refugee camps in Sudan were filling up so quickly that the mode of rescue had to be revamped.[15]

Israeli officials approached the United States for assistance, but the request created a major dilemma because unlike Israel, which was technically at war with Sudan, the United States enjoyed very close relations with President Gaafar al-Numeiry. Accordingly, the United States provided Sudan with large amounts of aid and subsequently exercised leverage over Numeiry. In 1984, Numeiry was in urgent need of further U.S. aid because of Sudan's failing economy, civil unrest, and the need to take care of the nearly half a million refugees, the majority of whom were non-Jews. The problem was that as a member of the Arab League, Numeiry could not afford to be seen to be helping the "Zionists." U.S. officials were well aware of Sudan's instability and were hesitant to do anything that might further endanger Numeiry's regime.

A Sudanese representative traveled to the United States in June 1984 to ask for additional economic aid. In a meeting with Richard Krieger and Eugene Banks of the State Department, Krieger decided to play on his visitor's anti-Semitic feelings; he suggested that the approval of the omnipotent Jewish lobby would be necessary to obtain congressional support for an increase in aid and suggested that Sudan could help by allowing the United States to take the Ethiopian Jews out of

the refugee camps. The Sudanese official found this line of argument appealing, and moves were made to arrange a rescue operation. The Refugee Affairs Co-ordinator at the U.S. embassy in Khartoum, Jerry Weaver, met with Sudanese vice president and security chief Omar Tayeb and secured his agreement to a plan for evacuating the Ethiopian Jews.

According to the plan, the Mossad and the Sudanese secret police would devise the secret operation, known later as Operation Moses. It lasted from November 21, 1984, to January 5, 1985. Altogether 7,800 Ethiopian Jews were rescued in this manner. However, as news of the airlift leaked out, the Sudanese ordered a halt to the operation. As an Arab country, Sudan would not allow its image in the Arab world to be tarnished by way of assisting in enlarging the Jewish population in Israel.[16]

U.S. officials considered the resumption of Operation Moses. On March 3, 1985, Vice President George H.W. Bush met with Numeiry. The latter was reluctant to resume the operation and instead agreed to a quick, one-time secret U.S. (not Israeli) operation in which the flights would not go directly to Israel. The result was that the United States released to Sudan, within a week, US$15 million out of $200 million promised. The remainder was remitted later. To avoid any possibility of disclosure, President Ronald Reagan wanted the operation to be carried out within three or four days. The CIA Station chief in Khartoum thus took an embassy plane to reconnoiter the runway of a remote airstrip near Gedaref and found that it was fit for landings and take-offs.[17]

On March 28, 1985, Operation Sheba began, with Israeli Ethiopian Jews working for Mossad identifying the Ethiopian Jews in the camps and bringing them by truck to the airstrip, eight miles outside Gedaref. Six U.S. Hercules airplanes loaded with food and medical supplies departed to Sudan from a U.S. airbase near Frankfurt, Germany, and landed at twenty-minute intervals to pick up the remaining Ethiopian Jews. However, instead of flying to intermediate destinations, the airplanes flew directly to an Israeli air force base near Eilat, in southern Israel. The original plan of Operation Sheba was to rescue as many as 2,000 Ethiopian Jews from the camps, but they found only 494.

After Operation Sheba concluded, the Israeli government believed that all of the Ethiopian Jews had been evacuated from the refugee camps in Sudan. In fact, many were left, mainly the old and infirm. Soon after Operation Sheba came to an end, Numeiry was overthrown and found asylum in Cairo. The former Sudanese Vice-President Tayeb and other officials were imprisoned or executed for allowing the Ethiopian Jews to leave Sudan for Israel. In sum, out the approximately 76,000 people of the Ethiopian Jewish community, 16,975 were taken to Israel during the 1980s.

Operation Solomon, known in Hebrew as Mivtza Shlomo, was another attempt at the beginning of 1990 at rescuing Jews from Ethiopia. Despite the rescue operations in the 1980s, many Jews still remained in Ethiopia, with numerous families having been divided. Following the resumption of diplomatic relations between Israel and Ethiopia in early 1990, thousands of Jews flocked to the

compound around the Israeli embassy in Addis Ababa awaiting their turn to be evacuated to Israel. In 1990 the Mossad embarked on a complex and politically sensitive mission, code-named Operation Solomon, to airlift thousands of Jews from Ethiopia to Israel. The Israeli government had reached an agreement with Ethiopia's ruler, Col. Mengistu Haile Mariam, to allow their departure for US$30 million. On May 24, 1991, with Ethiopian antigovernment rebels closing in on the Ethiopian capital, Operation Solomon was activated and lasted for thirty-three hours, evacuating some 14,325 Ethiopian Jews. The Mossad, which had a key role in the operation, had been assisted on the ground in Ethiopia mainly by Wonderferer Aweke, an Ethiopian Jew.[18]

THEFT OPERATIONS

Soon after Meir Amit's appointment as director of the Mossad on March 25, 1963, he met with many commanders in the IDF to clarify the Mossad's objectives. He asked what they thought could be the Mossad's most valuable contribution to Israeli security. Maj. Gen. Ezer Weizman, then commander of the Israel Air Force (IAF), remarked that bringing a Soviet-made MiG-21 to Israel would contribute the most to Israeli security. Israel would then have access to the secrets of the most advanced fighter planes the Arab states possessed and, according to the Russians, the most advanced strike aircraft in the world.[19]

The Soviet Union began introducing the MiG-21 into the Middle East in 1961 under heavy secrecy. By 1963 this aircraft had become the major aircraft of the air forces of Egypt, Syria, and Iraq. Few in the West knew much about the MiG-21, but all feared its capabilities. The Mossad had tried unsuccessfully twice to bring a MiG-21 to Israel, and proverbially the third attempt paid off from an unexpected source with little prompting from Israeli intelligence. An Iraqi Jew called Yusuf contacted Mossad officers with somewhat curious information that he might be able to arrange the theft of a MiG-21.

Yusuf had been born to an impoverished Jewish family in Iraq and became an indentured servant to an Iraqi Maronite Christian family at age ten. Although he never attended school and was illiterate, he, not unlike the biblical Joseph, rose to prominence in this family's household. When he was almost sixty, however, the head of the household told Yusuf during a quarrel that without the family he would have had nothing, a taunt Yusuf would not forget. He decided then and there to explore his "otherness"—his Jewish identity, something he had hardly given a thought to. In 1964 he contacted Israeli officials in Tehran (until 1979 Israel had sound relations with non-Arab Iran) and in Europe.

Through Yusuf, Israel made contact with a Maronite Christian pilot in the Iraqi air force, whose family felt the pressure of their Maronite Christian coreligionists under Muslim authoritarian rule. In a previous conversation with Yusuf, the pilot mentioned he would like to leave the country, and this was reported by Yusuf to the Israelis. An American woman, an agent for the Mossad in Baghdad,

was assigned to draw out Munir Redfa, an Iraqi Christian air force pilot and a member of Yusuf's adoptive family. The two bonded well, and several salient points were mentioned by Redfa: his disagreement with the war waged by his government against the Kurdish minority in northern Iraq, the fact that although he was a squadron commander he was stationed far from his home in Baghdad, and that because of to his Christian beliefs he was only allowed to fly with small fuel tanks. Furthermore, he commented on his admiration for the Israelis: the few against so many Muslims.

The female agent developed the relationship and suggested they take a holiday together in Europe in July 1966. After a few days of vacation, she suggested to Redfa that he fly with her to Israel, adding that she had friends there who might assist him. Despite initial disquiet from Redfa, the couple arrived in Israel and Redfa was given VIP treatment. After assessing the matter, Redfa was offered Israeli citizenship and US$1 million, an offer he accepted on condition that the Mossad arrange for the escape of his entire family from Iraq as well: his wife, his children, and his parents, along with the rest of his extended family.

The new commander of the IAF from April 1966, Maj. Gen. Mordechai Hod, met Redfa to plan the dangerous MiG flight together. All that remained for Redfa was to fix the date for his flight, which he set for August 16, 1966.

Soon members of Redfa's family began leaving Iraq for a variety of reasons. On that day in August, Redfa went about his business in Iraq as usual, and requested that the ground crew fill his tanks to capacity, an order the Russian advisors generally had to countersign. But the Iraqis disliked the Russian advisors, who seemed to hold them in contempt. This worked to Redfa's benefit, and he took off on his dangerous mission, knowing his fellow pilots would be ordered to shoot him down once Iraqi ground control realized he had diverted from his flight plan. Iraqi ground crew radar picked up a blip on the screen heading west, and they frantically radioed Redfa to turn around, warning he would be shot down. Hundreds of miles away Israeli radar picked up the blip on their screen, and sent a squad of IAF Mirages to escort him, while Redfa went through his prearranged signals, eventually meeting up with the Israeli fighter pilots who escorted him to a base deep in the Negev Desert, in the south of Israel.

On the same day, Mossad agents in Iraq picked up all the remaining members of the pilot's family, who had left Baghdad ostensibly for a picnic, and smuggled them out of the country. Newspapers all over the world carried the sensational story of an Iraqi pilot who had defected with his MiG-21 to Israel. It was no surprise when, during the Six-Day War in June 1967, the IAF demonstrated its superiority over the MiG-21 aircraft of the Arab air forces.

Operation Noah's Ark was the second "theft" covert operation, which involved the "stealing" of five missile boats Israel had ordered and paid for from the French shipyard at Cherbourg at the end of 1969. In 1962, Israel placed an order for missile boats with West German shipyards, as part of the reparations agreement between the two countries. Chancellor Adenauer agreed that the shipyards would build twelve missile boats for the Israeli navy on condition that the

transaction be kept secret so as not to incur the wrath of the Arab world. By the end of 1964, three of the twelve missile boats had been built and delivered. However, certain members of the West German government leaked news of the deal to the *New York Times*, with the result that the missile boats would still be financed by the reparations scheme but would be built outside West Germany. The contract for building the remaining boats was given to the Cherbourg shipyards in Normandy on the northern coast of France. In April 1967, the first of the nine boats was delivered to the Israeli navy, and a month later Israel received the second vessel, accumulatively the fifth boat in the purchasing contract.[20]

During the crisis on the eve of the 1967 Six-Day War, on June 2 French President Charles de Gaulle declared that France would no longer supply offensive weapons to the Middle East, which in real terms meant that Israel was to suffer a disadvantage, as the Arab world was being supplied by the Soviet Union. However, since the building of the missile boats in the Cherbourg shipyards was considered a contract in progress, two more boats were delivered to the Israeli navy in the fall of 1967.

Following a Palestinian terror attack on an Israeli aircraft at Athens airport on December 26, 1967, and the Israeli retaliation against Beirut airport two days later with the blowing up of thirteen Lebanese airplanes on the ground, de Gaulle declared that the French arms embargo would now be absolute, including the Cherbourg boats, despite the fact that they had been paid for.

On January 4, 1969, a week after de Gaulle's announcement, small teams of Israeli naval officers and sailors made their way to France and boarded three more missile boats that were almost complete. They spent three hours completing the vessels for sail, after which they hoisted the Israeli ensign and set off. They moved into the English Channel and never returned.

But Israel still desired the remaining boats and, in November of 1969, the clandestine Operation Noah's Ark was implemented. The Israeli Maritime Fruit Company registered the fictitious Starboat Line. A few days later, the Israeli navy informed Cherbourg shipyard management that the Israeli government had decided to seek compensation from the French government for breaching the agreement to deliver the boats to Israel; Israel would concede the boats. Renowned Norwegian shipping expert Ole Martin Siem was invited to join Starboat's board of directors for the specific purpose of purchasing the missile boats. On November 11, 1969, the France-based Israeli coordinator of the naval purchase, Israeli navy reserve Rear Adm. Mordechai Limon, received an acceptable compensation offer from the Cherbourg officials, whereupon Limon gave the go-ahead to Siem for the fictitious purchase of the missile boats.

Shortly thereafter, Siem met the French government's arms vendor, Gen. Louis Bone, and told him that he had heard that several missile boats were for sale and they might be converted to drill for oil. The French general agreed to the sale. One hundred twenty Israeli seamen entered France in pairs as the next stage of the operation and surreptitiously prepared the vessels. On Christmas Eve 1969,

despite the unstable weather conditions, final checks were carried out with the boats, which departed France on Christmas Day for Israel.

On December 26, the French authorities realized what had just happened. Although the Israeli government did not admit responsibility for the affair, Limon, who had lived in France for seven years, was declared persona non grata by the French authorities and ordered to leave. Two French generals were dismissed for their part in approving the sale of the missile boats to the fictitious Starboat Line. Seven days after leaving Cherbourg, the missile boats were anchored in Israel.[21]

OPERATIONS ISORAD AND PLUMBAT

For the purpose of secretly obtaining uranium for the Israeli nuclear reactor in Dimona in the 1960s, Israel used the services of the American company Nuclear Material and Equipment Corporation (NUMEC), a Pennsylvania-based manufacturer of nuclear fuels and specialty metals. For this purpose a dummy company, Isotopes and Radiation Enterprises (ISORAD), was formed in the United States.

During Operation Isorad, Dr. Zalman Shapiro, president of NUMEC, succeeded in diverting large quantities of weapons-grade uranium to Israel. In those years the unaccounted-for uranium missing from NUMEC's plant sparked the curiosity of the American federal authorities, and NUMEC paid almost US$930,000 in fines.[22]

Operation Plumbat, also known as the Uranium Ship Operation, was another covert operation related to stealing uranium. This was a joint operation of LAKAM and the Mossad, in support of the Israeli nuclear weapons effort. A West German chemical corporation named Asmara had bought uranium through subsidiaries from a Belgian company, Société Générale de Mianro. The uranium was loaded in Antwerp onto the vessel *Scheersberg A*. According to the manifest, the ship and its cargo was bound for Genoa. Entering the Mediterranean, the ship sailed east instead of south according to its declared destination, and somewhere between Cyprus and Turkey it rendezvoused with an Israeli freighter chartered by the Mossad. The cargo of some 200 tons of yellow cake uranium in 560 oil drums labeled "Plumbat" (lead) was smuggled onto the Israeli freighter.[23]

The *Scheersberg A* then simply disappeared for a couple of days, showing up later at Iskenderun (a port in Turkey) where the cargo was discovered to be missing. The West German government may well have been directly involved, but if so, this fact remained under wraps to avoid antagonizing the Soviets or the Arabs.[24]

THE IRANGATE AFFAIR

Israel, along with the United States, suffered a grave loss with the fall of the shah of Iran at the end of 1979. The Israeli leaders assumed that consistent

geopolitical interests would eventually triumph over religious ideology and produce an accommodation between Israel and Iran. The onset of the Iran-Iraq war in 1980 gave Israeli leaders the incentive to keep their door open to the Islamic rulers in Iran. The director general of Israel's Foreign Ministry, David Kimche, recommended selling arms to relatively moderate Iranians in positions of power, such as Ayatollah Ali Akbar Hashemi Rafsanjani. His comments were echoed by Uri Lubrani, Israel's chief representative in Iran under the Iranian leader, Shah Pahlavi. The Israeli Defense Minister, Reserve Gen. Ariel Sharon, also supported the idea and believed that Israel's vital interest was a continuation of the war in the Persian Gulf, with an eventual Iranian victory.[25]

The head of the Jaffee Center for Strategic Studies at that time, Aharon Yariv, a retired major general and former director of MI, stated at a scholarly conference at Tel Aviv University in late 1986 that it would be to Israel's advantage if the Iran-Iraq war ended in a stalemate, but it would be even more advantageous for Israel if the war continued. The salient understanding was that once the war ended, Iraq may open up an "eastern front" against Israel.

The first renewed Israeli arms sales to Iran in 1980 included spare parts for U.S.-made F-4 Phantom jets; a later deal that year included parts for U.S.-made tanks, and Israeli officials only informed Washington after the fact, because they believed that the United States would not grant upfront approval of such transactions. The administration of Jimmy Carter was outraged that its embargo had been blatantly violated by the Israelis, especially in light of the hostage crisis with which the United States was being confronted by the Iranians. This had erupted in November 1979 in the early days of the revolution, when Iranian radicals seized the U.S. embassy in Tehran and took sixty-six American diplomats hostage. Thereafter, and until the diplomats were released in January 1981, U.S. Secretary of State Edmund Muskie demanded that Israel cease its shipments.

Israeli Prime Minister Begin promised to comply with the U.S. demands, but in fact Israel continued to sell arms to Iran without U.S. approval. On July 24, 1981, Ya'acov Nimrodi, an Israeli businessman and longtime associate of Ariel Sharon, signed a deal with Iran's Ministry of National Defense to supply arms worth US$135,842,000, including Lance missiles, Copperhead shells, and Hawk missiles. A sale of such a magnitude must have had Israeli government acquiescence. President Reagan's administration took office in 1981 and, toward the end of that year, Kimche approached U.S. Secretary of State Alexander Haig and National Security Adviser Robert McFarlane to discuss proposed Israeli shipments of U.S.-made spare parts worth $10–15 million to a relatively moderate faction in Iran. Haig disapproved the request. In November 1981, Ariel Sharon visited the United States and requested approval from his counterpart, Caspar Weinberger, to sell arms to Iran. Weinberger deferred the decision to Haig, who rejected the request outright. In May 1982 a clandestine gathering took place between Al Schwimmer (an American Jewish billionaire who had founded the Israeli aircraft industry), Nimrodi, Kimche, and Sharon and his wife, Lily, together with Sudanese President Gaafar Numeiry, at a Kenyan safari resort owned

Table 3-1. Categorization of Covert Operations: Commonly Used Names of the Various Operations That Have Been Used for Practical Purposes

PLANNED TO BE TOTALLY COVERT	COVERT FOR TACTICAL REASONS	COVERT YET BEARING ISRAELI FINGERPRINTS
The Bad Business*	Entebbe†	Abu Jihad†
Khaled Mashal fiasco*	Moses†	The Engineer*
Wrath of God*	Solomon†	Damocles*
Irangate*	Sheba†	ISORAD*
	MiG-21*	Plumbat*
	Spring of Youth*	
	Blanket*	
	Cherbourg Missile Boats†	
	Noah's Ark†	

*Nonmilitary.

†Paramilitary. For the purpose of this chapter, *paramilitary* means *auxiliary* military, that is, something not quite military performing military duties. There are political connotations to the term *paramilitary* that often override the original meaning, hence there are contradicting understandings of the term. Those political connotations, however, are localized and at times may again be contradictory. There are paramilitary units that carry out paramilitary activity that are an officially legislated arm of the government. Paramilitary actions carried out by such groups can serve many different functions.

by Saudi business tycoon Adnan Khashoggi. At the meeting, Israel won Numeiry's agreement to allow Ethiopian Jews safe passage through Sudan to migrate to the Jewish state, and in return Numeiry requested Israel's assistance in evacuating him from his country should his regime be toppled

Under U.S. pressure, Israel halted arms sales for a short period, but private Israeli citizens, including Nimrodi, continued making plans to resume trade ties with Iran. In 1985 Nimrodi succeeded in obtaining approval for his plans from Israel's national unity government headed by Shimon Peres. Nimrodi and his partner Schwimmer, a close friend of Peres, were authorized to provide Iran with Lau antitank missiles and antiaircraft Hawk missiles from Israel's stockpiles. These deals were part of what was later known as Irangate—half of the Iran-*contra* affair revealed in 1986.

In the mid-1980s, Schwimmer played a key role in persuading the U.S. administration itself to sell arms to Iran. Through a secret agreement between the United States and the Israeli Defense Ministry in 1985, the arms went to Iran via Nimrodi, with the United States replenishing the supplies Israel transferred to the Iranians. One aspect of the deal was that Iran was to exert pressure on its protégé, the Hezbollah organization in Lebanon, to release U.S. and Western hostages kidnapped after 1982. The Reagan administration was fully aware of attempts at freeing the hostages by means of unsanctioned arms sales to Iran.

News of Irangate, or as it was more commonly known, the Iran-*contra* affair, first began appearing in the media toward the end of 1986. It revealed how deeply

the United States was involved in arms sales to Iran, breaching its own laws. One law prohibited the sale of U.S. weapons for resale to a third country listed as a terrorist nation, and this occurred precisely at a time when the Washington was publicly calling for a worldwide ban on selling arms to Iran. Moreover, the monies paid by Iran for the U.S. arms were redirected by senior officials in the Reagan administration to buy arms for the *contra* rebels in Nicaragua. This went against the Boland Amendment of December 8, 1982, which specifically prohibited military assistance to the *contras*. One of the administration officials involved in the scandal was Lt. Col. Oliver L. North, military aide to the National Security Council, who reported in the White House to Robert McFarlane and later to his successor, Vice Adm. John M. Poindexter. The entire scheme was conducted without Congress's knowledge, again contravening a law requiring sales above US$14 million to be reported to Congress.[26]

CONCLUSION

Although not all of the Israeli covert actions and clandestine collection operations discussed here were carried out in a clandestine manner, of those in the public domain, the most widely known were operationally executed under varying levels of secrecy. In reviewing several of the literally hundreds of diverse covert missions carried out by the different branches of the Israeli intelligence community, it becomes clear that in defense of the homeland, the style and type of operation selected is only limited by the imagination of those involved.

NOTES

1. Aviezer Golan, *Operation Susannah* (New York: Harper & Row, 1978).
2. Ephraim. Kahana, *Historical Dictionary of Israeli Intelligence* (Lanham, MD: Scarecrow Press, 2006).
3. "The Bungle in Jordan: Mossad Trips Up during an Attempted Hit on a Hamas Leader," *Time*, October 13, 1997.
4. Kahana, *Historical Dictionary of Israeli Intelligence.*
5. Alexander B. Calahan, "Countering Terrorism: The Israeli Response to the 1972 Munich Olympic Massacre and the Development of Independent Covert Action Teams," master's thesis, Marine Corps Command and Staff College, 1995.
6. George Jonas, *Vengeance: The True Story of an Israeli Counter-Terrorist Team* (London: Simon & Schuster, 1984).
7. Kahana, *Historical Dictionary of Israeli Intelligence.*
8. Ibid.
9. Ian Black and Benny Morris, *Israel's Secret Wars: A History of Israel's Intelligence Services* (New York: Grove Press, 1991).
10. Kahana, *Historical Dictionary of Israeli Intelligence.*

11. Yeshayahu Ben-Porat, Eitan Haber, and Zeev Schiff, *Entebbe Rescue*. Transl. Louis Williams (New York: Delacorte, 1977).

12. Kahana, *Historical Dictionary of Israeli Intelligence.*

13. Ibid.

14. Ibid.

15. Claire Safran, *Secret Exodus: The Story of Operation Moses* (New York: Prentice Hall, 1987).

16. Kahana, *Historical Dictionary of Israeli Intelligence.*

17. Ibid.

18. Melissa Crow, *Operation Solomon: A Case Study on the Role of Power Politics in International Negotiation*. Working Paper Series 92-10. Cambridge, MA: Harvard Law School, Program on Negotiation, 1992.

19. Kahana, *Historical Dictionary of Israeli Intelligence.*

20. Ibid.

21. Abraham Rabinovich, *The Boats of Cherbourg: The Secret Israeli Operation That Revolutionized Naval Warfare* (New York: Seaver Books, 1990).

22. Kahana, *Historical Dictionary of Israeli Intelligence.*

23. Elaine Davenport, *The Plumbat Affair* (Philadelphia: J. B. Lippincott, 1978).

24. Kahana, *Historical Dictionary of Israeli Intelligence.*

25. Fred Halliday, *Beyond Irangate: The Reagan doctrine and the Third World* (Amsterdam: Transnational Institute, 1987).

26. Kahana, *Historical Dictionary of Israeli Intelligence*.

4

"SUCH OTHER FUNCTIONS AND DUTIES"

Covert Action and American Intelligence Policy

JAMES M. SCOTT AND JEREL A. ROSATI

ALTHOUGH THE U.S. GOVERNMENT HAS EMPLOYED COVERT operations since the time of the American Revolution, World War II marks the point at which such activities became a major element of U.S. security policy. Building on the activities of the Office of Strategic Services (OSS) in World War II, U.S. policy makers first established the Central Intelligence Group in January 1946 (by executive order), and then, about eighteen months later, the Central Intelligence Agency (CIA), through the National Security Act. Among other things, the 1947 National Security Act charged the CIA with a variety of intelligence gathering and analysis functions, as well as "such other functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct." This ambiguous language was the only indication in this seminal legislation that the CIA would be engaged in covert action. Over time, of course, covert action became a signature activity of the agency and perhaps the most controversial as well. In fact, it was only days after the passage of the 1947 act that the Truman administration authorized a series of propaganda activities in Europe.[1] From this relatively modest start, covert action and the CIA's role in it grew considerably.

This chapter reviews the use of covert action in U.S. foreign policy since World War II, focusing on the methods that have been employed over time. After a discussion of the definition of covert action, it surveys covert actions through several periods from the end of World War II until the present. Following this brief overview, the chapter then discusses the range and methods of covert action and concludes by reflecting on key dilemmas associated with the use of covert action as a foreign policy instrument.

COVERT ACTION

Covert action has often been characterized as the "middle option," "third way," or "quiet approach" to be used when doing nothing and using force are both unacceptable. Accordingly, as other observers have noted, it has more to do with a method than with any particular actions. Indeed, according to Berkowitz and Goodman, almost every activity that has been typically considered a covert action has also been conducted overtly.[2] Hence, what constitutes covert action is somewhat elusive.

As already noted, the 1947 National Security Act mentioned only "such other functions and duties." In mid-1948, George Kennan authored a policy document—NSC 10/2—that characterized covert action as those activities "so planned and conducted that any U.S. government responsibility for them is not evident to unauthorized persons and that if uncovered the U.S. government can plausibly disclaim any responsibility for them."[3] In 1978, President Jimmy Carter issued an executive order that defined covert action as

> operations conducted abroad in support of national foreign policy objectives which are designed to further official United States programs and policies abroad and which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but not including diplomatic activity or the collection and production of intelligence or related support functions.[4]

Just a few years later, Ronald Reagan's Executive Order 12333 essentially restated this definition, adding that covert actions "are not intended to influence United States political processes, public opinion, polices, or the media and do not include diplomatic activities or the collection or production of intelligence and related support functions."[5] The essence of these definitions was captured in the 1991 Intelligence Authorization Act, which defined covert action as "activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[6]

The National Clandestine Service (NCS), the modern-day name for what has been known as the Office of Policy Coordination, the Directorate of Plans, and then the Directorate of Operations, is primarily responsible for U.S. covert operations. The NCS actually involves three types of activities: espionage, counterintelligence, and covert action. Espionage involves human intelligence, such as running spies and double agents abroad to access information, and counterintelligence emphasizes preventing foreign intelligence agencies from penetrating the CIA. Covert actions, by contrast, are influence operations.[7]

A core element of covert action is obviously that the U.S. government conceals its responsibility. As Berkowitz and Goodman have noted, there are two main justifications for such subterfuge: "one is when open knowledge of U.S.

responsibility would make an operation infeasible . . . the other valid reason . . . is to avoid retaliation or to control the potential for escalation."[8] In either case, covert action is fundamentally a foreign policy option, not an intelligence activity.[9] As Loch K. Johnson has noted, "whatever the variation in terminology, the objective of covert action remains constant: to influence events overseas secretly and in support of U.S. foreign policy."[10] As the following historical overview suggests, the use of covert action as a foreign policy instrument has been closely tied to the overarching foreign policy ethos of the time.

COVERT ACTION SINCE WORLD WAR II: AN OVERVIEW

From its creation until the collapse of the Soviet Union, the CIA and its covert operations have evolved through four stages: (1) the "good old days," 1947 through the early 1970s; (2) the "fall" and reform, early 1970s to 1979; (3) the resurgence, during the 1980s; and (4) the adjustment, in the post–Cold War and post–September 11, 2001, periods.[11]

The Good Old Days, 1946–73

In terms of budget, personnel, and missions, the CIA grew quickly in the late 1940s and 1950s. All the agency's bureaucratic directorates and functions expanded, but none more so than the operations directorate. Initially, extensive covert operations were probably not envisioned; many observers, including Clark Clifford, George Kennan, Sidney Souers, and President Harry Truman, commented later that the CIA's covert action mission grew well beyond what was imagined at its inception.[12] The CIA was created to provide the president with an intelligence capability to engage in data collection and analysis as well as coordinate the larger intelligence community existing at the time. However, as suggested, one clause of the CIA charter allowed it to "perform such other functions and duties," which provided the later legal justification for involving the CIA in cloak-and-dagger operations.[13] Over time, the CIA soon became the major governmental organization responsible for covert actions abroad in support of the policy of containment.

The rise of the Cold War was the essential factor prompting the growth of the covert action mission. Estimates are that the vast majority of the CIA's budget and personnel throughout the Cold War were devoted to operations. According to Johnson, for example, by the mid-1960s, more than 60 percent of the CIA's budget was dedicated to covert action.[14] The president used the CIA to perform various covert activities that no other agency performed and that were officially denied in public. In fact, the CIA was allowed considerable independence in running its covert operations under presidential supervision.

Although extensive operations were initiated in Europe in the years after World War II, including information campaigns, the provision of political support to preferred parties and individuals, subversion, and other activities, the heyday of covert operations occurred under Director Allen Dulles from 1952 to 1961, a time when his brother, John Foster Dulles, also served as secretary of State.[15] Even though the president often remained distant from the details of an operation, the director responded to presidential initiative and choice. Also, no real oversight existed outside the executive branch, as Congress generally preferred to remain on the sidelines in deference to presidential leadership and the Cold War consensus.[16]

Prevailing Cold War attitudes help explain the vital role that covert action came to play in U.S. foreign policy. American leaders saw a world divided between the forces of good and evil—the free world represented by the United States against the totalitarian, communist bloc represented by the Soviet Union. The Soviet Union was also seen as aggressive, expanding its territorial control and directly threatening American interests and the status quo. Consequently, American policy makers were preoccupied with rearming and creating alliances to deter Soviet expansionism and, if deterrence failed, to fighting a "hot" war. At the same time, American policy makers increasingly came to rely on covert operations to fight the "Cold" War. Such measures were justified in terms of an anticommunist philosophy and a strategy of power politics, in which the ends justifies the means. A secret report authored by Gen. James Doolittle for the 1954 Hoover Commission captured the perspective nicely:

> It is now clear that we are facing an implacable enemy whose avowed objective is world domination by whatever means at whatever cost. There are no rules in such a game. Hitherto acceptable norms of human conduct do not apply. If the U.S. is to survive . . .We must learn to subvert, sabotage and destroy our enemies by more clever, more sophisticated and more effective methods than those used against us. It may become necessary that the American people will be made acquainted with, understand and support this fundamentally repugnant philosophy.[17]

Driven by this perspective, the CIA became an important tool of U.S. foreign policy immediately after its creation in 1947. The examples discussed next highlight just a few of the important covert activities abroad, which include: (1) manipulating foreign democratic elections; (2) organizing partisan resistance movements; (3) overthrowing foreign governments; (4) participating in foreign assassinations; (5) supporting friendly, often authoritarian governments; and (6) training foreign military, intelligence, and police personnel.

It has been reported that by 1953 the CIA had major covert operations in progress in forty-eight countries.[18] A U.S. Senate select committee investigating foreign and military intelligence in 1975 found that the CIA had "conducted some 900 major or sensitive covert action projects plus several thousand smaller projects since 1961."[19] In other words, the CIA, in its heyday, was engaged in

covert operations all over the world, with as much as one-third of its interventions taking place in "pro-Western" democracies.[20] Table 4-1 highlights some of the major covert operations during the "good old days" that have come to light, although much CIA covert activity remains unknown.

In the years after World War II, one frequently employed type of covert activity of the CIA involved influencing foreign elections. In both Italy and France in 1948, for example, the United States worried that the economic and political instability after the war, which strengthened legal communist parties in those countries, would eventually result in communist electoral victories. Consequently, the CIA engaged in a variety of efforts to undermine the communists and strengthen the centrist parties. In Italy, for example, the agency funded and supported the Christian Democratic Party and distributed propaganda and disinformation through a network of Italian media assets (paid agents) employed throughout the print and electronic media to discredit the Communist Party. The Christian Democrats won the election, although the extent of CIA influence remains unclear.

In the late 1940s and 1950s, the CIA also supported partisan resistance movements in communist countries to promote internal instability and domestic uprisings. For example, the agency trained émigrés and secretly transported them into Albania, Poland, Yugoslavia, the Baltic states, Soviet Georgia, and the Ukraine. These partisan resistance efforts made very little headway; in fact, in most cases they were speedy failures. For example, the fairly extensive effort in Albania persisted for a number of years until it became clear that the communist regime had infiltrated the resistance and virtually all the agents had been apprehended almost immediately.

Under President Eisenhower, the CIA became involved in a series of efforts to overthrow foreign governments. For example, with help from the British MI6 (their CIA equivalent), the CIA staged the Iranian coup of 1953 to overthrow the nationalist leader Mohammed Mossadeq and restore the Pahlavi dynasty, headed by the shah. Mossadeq had proclaimed an independent and neutralist state in the growing Cold War and demanded that Great Britain renegotiate its most favorable contract for Iranian oil, and U.S. policy makers feared he was playing into the hands of the communists and the Soviet Union. Once restored, the shah subsequently awarded Gulf, Standard of New Jersey, Texaco, and Socony-Mobil a 40 percent share of Iranian oil rights.[21]

A year later, the CIA staged the 1954 coup in Guatemala, which became the model for many of the agency's subsequent actions. With a history of dictatorial rule, in 1950 Guatemala experienced its first taste of democracy when Jacobo Arbenz Guzmán was elected president. However, when Arbenz promoted agrarian reform and expropriated 234,000 acres of uncultivated land owned by the United Fruit Company, an American company that owned over 40 percent of Guatemalan territory, U.S. policy makers, including President Eisenhower and Secretary of State Dulles, concluded that the Arbenz regime was "playing the communist card" and posed a threat to American national security. The CIA thus

Table 4-1. Major CIA Covert Operations During the "Good Old Days"

1947–48	Propaganda campaign during the 1948 Italian national elections
1947–48	Propaganda campaign during the 1948 French national elections
1948–52	Partisan resistance movements in Eastern Europe and Soviet Union
1949	Anglo-American effort to overthrow the Albanian government
1950–70s	Propaganda campaigns through Radio Liberty and Radio Free Europe
1952–60	Kuomintang Chinese partisan resistance movement on Sino-Burmese border
1953	Anglo-American overthrow of Prime Minister Mohammed Mossadegh of Iran
1953–54	Campaign to support Ramon Magsaysay's presidential candidacy and counter Huk insurgency in the Philippines
1954	Overthrow of President Jacobo Arbenz of Guatemala
1950s–70s	Subsidization of domestic and foreign groups and publications
1953–70s	Drug testing and mind-control program
1954–70s	Effort to overthrow leader Ho Chi Minh and the North Vietnamese government
1955	Effort to destabilize President José Figueres's government of Costa Rica
1958	Support of Tibetan partisan resistance movement in China
1958–65	Effort to destabilize President Sukarno of Indonesia
1960	Alleged effort to assassinate Gen. Abdul Kassem, leader of Iraq
1960	Alleged effort to assassinate President Abdul Nasser of Egypt
1960	Alleged effort to assassinate political leader Patrice Lumumba of Congo
1961	Effort to overthrow Fidel Castro, leader of Cuba
1961	Effort to assassinate Rafael Trujillo, leader of Dominican Republic
1961	Effort to destabilize President Kwame Nkrumah of Ghana
1960s	Effort to assassinate Fidel Castro of Cuba
1960s	Fought secret war in Laos
1962–63	Destabilized the Ecuadorean governments of Ibarra and Arosemena
1963	Destabilized Prime Minister Cheddi Jagan's government of British Guiana
1963	Supported overthrow of President Ngo Dinh Diem of South Vietnam
1960s	Conducted pacification and Phoenix programs in Vietnam
1964	Campaign in support of President Eduardo Frei in 1964 Chilean elections
1964	Supported military coup against President Joao Goulart of Brazil
1967	Supported military coup in Greece
1967–70s	Domestic campaign against antiwar movement and political dissent
1970–73	Destabilized Chilean government of President Salvador Allende

Sources: Rhodri Jeffreys-Jones, *The CIA and American Democracy* (New Haven, CT: Yale University Press, 1989); Jonathan Kwitny, *Endless Enemies* (New York: Penguin, 1984); Thomas Powers, *The Man Who Kept the Secrets* (New York: Pocket Books, 1979); John Prados, *Presidents' Secret Wars* (New York: William Morrow, 1986); John Ranelagh, *The Agency* (New York: Simon & Schuster, 1986); David Wise and Thomas B. Ross, *The Invisible Government* (New York: Vintage, 1974); U.S. Congress, Senate, *Alleged Assassination Plots Involving Foreign Leaders*, Congressional Report, 94th Congress, 1st sess. (November 18, 1975); and U.S. Congress, Senate, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, Books 1–6, Congressional Report, 94th Congress, 2nd sess. (April 14, 1976).

trained several hundred Guatemalans on a United Fruit plantation in neighboring Honduras and, when it sent the unit into Guatemala, waged an extensive information and psychological warfare campaign to make the force appear larger. The CIA also piloted several small planes in a bombing run over Guatemala City and other key towns. Arbenz lost his nerve and fled the country, and Castillo Armas became the new military dictator.[22]

In the 1950s and 1960s, the CIA also began to be involved in efforts to assassinate foreign leaders, although it appears that the agency was never actually successful in such attempts. For example, during the 1960 independence crisis in the Congo, it is alleged that the CIA attempted to assassinate the first prime minister and nationalist African leader, Patrice Lumumba, who was perceived as being too independent of American interests and open to communist subversion. The CIA was apparently unsuccessful, but Lumumba was assassinated eventually, clearing away for the U.S.–backed dictator, Mobutu Sese Seko, who ruled a corrupt regime for thirty years and impoverished the country.[23] In the 1960s, the CIA made numerous attempts to arrange the assassination of Cuban leader Fidel Castro, none of which came to fruition (see following for more discussion of the anti-Castro campaign).

The CIA also supported foreign governments allied to the United States in such places as Iran, Nicaragua, Cuba, and elsewhere, often participating in an allied government's violent repression of its own people. As George Kennan, in a report to Secretary of State Dean Acheson, stated as early as 1950: "We cannot be too dogmatic about the methods by which local communists can be dealt with. . . . Where the concepts and the traditions of popular government are too weak to absorb successfully the intensity of communist attack, then we must concede that harsh governmental measures of repression may be the only answer."[24]

For example, in Indonesia, after actively destabilizing President Sukarno, a prominent leader of the Third World nonaligned movement beginning in 1958, the CIA actively supported his successor after Sukarno's ouster. The CIA then assisted the new government of General Suharto in eliminating Indonesian Communist Party members and repressing all internal dissent, which included providing the Indonesian army with lists of people to be arrested and killed. Estimates of the number of Indonesians killed in the ruthless campaign range from 300,000 to as many as 1 million, with hundreds of thousands jailed without trial. In South Africa, the CIA supported the white apartheid regime, even providing the regime with a tip from a deep cover CIA agent which led to the August 5, 1962, arrest of Nelson Mandela, the underground leader of the African National Congress, the major force opposing the Afrikaner government and the system of apartheid.[25] Mandela remained imprisoned by the South African government until February 1990; after the transition to black majority rule, he became the first president of South Africa.

The CIA also frequently offered retainers to foreign leaders, putting them on the CIA payroll, and the agency frequently engaged in training of foreign intelligence personnel, including those engaged in covert operations. The armed

forces and the national police of many governments allied with the United States also were trained by U.S. military and government personnel. Thus, the U.S. government was heavily engaged in providing overt and covert support with billions of dollars of foreign assistance to friendly governments to ensure their security as part of America's larger campaign to fight the Cold War.

In the late 1950s and 1960s, the CIA relied on a variety of covert operations to be rid of Castro in Cuba. The initial operation was modeled on the 1954 Guatemalan operation. Hundreds of exiled Cubans were recruited and trained by the CIA in Honduras as an invasion force. In 1961, President John Kennedy supported the Bay of Pigs invasion, and the Cubans invaded with limited air cover provided by the CIA. Unlike the Guatemalan operation, however, the Bay of Pigs invasion was a complete failure. The actual invasion strategy was flawed to begin with, and Castro did not flee but used the Cuban military to destroy and capture the invading force. The Bay of Pigs fiasco was the first major CIA covert operation that became public, embarrassing the U.S. government and President Kennedy.[26]

From that point on, President Kennedy and his brother, Attorney General Robert Kennedy, mounted a vendetta against Castro, authorizing the CIA to use all means available to destabilize and assassinate him. The CIA went so far as to turn to the Mafia for assistance, for the Mafia maintained connections in Cuba forged in the days when they ran gambling casinos, before Castro took power. Yet the covert plans to assassinate Castro failed. Most were harebrained schemes that only James Bond could have pulled off, such as attempts to slip Castro the hallucinogen LSD via a cigar, give him a pen with a poison tip, explode clamshells while he dove in the Caribbean, and sprinkle his shoes with an agent to make his beard fall out and with it, according to the psychological warfare experts, his Latin machismo.[27]

Failures did not deter the CIA's involvement in covert operations, nor the president from relying on such operations as a major instrument of U.S. foreign policy. Thus the Americanization of the war in Vietnam not only led to a major overt military effort to keep South Vietnam independent of North Vietnamese communism but included major covert efforts in Vietnam, as well. The U.S. government, with the use of the CIA, supported President Ngo Dinh Diem beginning in 1954. When Diem became less effective and lost credibility as an independent leader of South Vietnam, the U.S. government backed a military coup against him in 1963. The CIA was very active in Vietnam. It trained members of the Meo and Hmong tribes to conduct military operations in support of the American war effort, including a secret war in Laos. It also conducted the infamous PHOENIX program, which targeted thousands of suspected Viet Cong and communist supporters for "neutralization." Not only were many innocent individuals jailed, but torture, terrorism, and assassination were also used as part of the PHOENIX operation.

The last major covert operation during the good old days occurred in the Chilean coup d'état during the Nixon administration. Although Chile had been a

democracy since the early 1960s, the Nixon administration worried that the electoral process would bring to power Salvador Allende, an avowed Marxist who believed in socialist democracy. The CIA attempted to influence the elections, but Allende won anyway. The United States then began a campaign to destabilize the Allende regime, highlighted by a CIA covert program to destabilize the Chilean economy and persuade the Chilean military to stage a coup. The military coup came in 1973 and installed Augusto Pinochet as the dictator of Chile for the next sixteen years.

Fall and Reform in the 1970s

Beginning with the Bay of Pigs fiasco through the 1960s, the CIA faced increasing scrutiny. Operations were less successful than in the 1950s and were being exposed in the media, creating embarrassment and controversy for the U.S. government and American people at home and abroad. The failure of Vietnam politicized segments of American society and contributed to the collapse of the anticommunist consensus. The domestic political environment became even more critical when the revelations of Watergate uncovered abuses of presidential power. In this new political climate, charges were made that the president had become too powerful and abused his office in the name of national security. The CIA was a special focus of attention and was accused of activities that were immoral, illegal, and counterproductive to the long-term interests of the American people.

A period of intense scrutiny ensued. President Gerald Ford appointed the Rockefeller Commission in 1975 to investigate the intelligence community and recommend reforms. But while the Rockefeller Commission was operating, President Ford and Secretary of State Henry Kissinger were supervising a major CIA covert operation in Angola. This involved funding, training, and equipping two independence forces that were battling a Soviet-backed force for control of Angola following the end of Portuguese colonialism. Ford and Kissinger tried to keep the operation secret, but when word of the Angolan operation leaked, Congress voted to abort it and began its own investigation of intelligence.[28]

The House and Senate each conducted major investigations of the intelligence community and covert operations. The Pike and Church Committee investigations (named after the chairman of each chamber's Foreign Relations Committee) led to the first public knowledge of the scale of covert operations conducted by the CIA. Most Americans were, to put it mildly, shocked to discover the degree to which their government was in the business of overthrowing democracies, conducting coups d'état, and planning political assassinations. In this political climate, the intelligence community, especially the CIA and covert operations, experienced a major decline. Under President Ford and to a greater extent under President Jimmy Carter, the CIA budget, personnel, and activities were cut, especially in the directorate of operations, and greater emphasis was placed on the intelligence side of the agency and its technological capabilities. During this time, over 1,800 covert operatives were fired or forced to take early

retirement, and most covert operations were cut, including major political and paramilitary programs.

Congress also asserted itself in oversight. For example, in the 1980 Intelligence Oversight Act it established new, permanent intelligence committees in both chambers and required the submission to Congress of a "presidential finding" explaining the need and nature of any covert actions. Presidential executive orders were issued that limited the kinds of covert operations the CIA could conduct, such as forbidding U.S. governmental personnel from becoming involved in political assassinations. Furthermore, the Freedom of Information Act, first passed in 1967, was strengthened to allow public access to classified information. The net impact was that the use of covert operations as a tool of U.S. foreign policy (and morale among covert operatives) reached its nadir by the end of the 1970s.[29]

The Resurgence of Covert Action in the 1980s

Beginning in 1980, the CIA and covert operations got a new lease on life. The resurgence of the agency began during the last year of the Carter administration, amid growing concern with the threat of the Soviet Union after its invasion of Afghanistan in December 1979. President Carter approved a major covert operation to send money and arms to the Afghan resistance forces through U.S.-controlled sources and agents in Pakistan and Saudi Arabia. Support to the Afghan resistance escalated under presidents Reagan and George H. W. Bush and continued into the early 1990s.[30]

It was under the Reagan administration, however, that the CIA and the use of covert operations became a major force in U.S. foreign policy reminiscent of the early Cold War days. William J. Casey, a strident anticommunist and former member of the OSS during World War II, was selected as Director of Central Intelligence (DCI). Under Casey, the CIA rejuvenated its operations division and rehired many former covert operatives.[31] Under Casey, the CIA again became active in combating communism abroad. The agency launched over a dozen "major" covert operations (defined by the congressional intelligence committees as an operation costing more than $5 million or designed to overthrow a foreign government) in places such as Central America, Angola, Libya, Ethiopia, Mauritius, Cambodia, Afghanistan, and Iran. Among the most significant of these was the huge CIA Afghanistan operation to support insurgents—known as the *mujahedeen*—against the invading Soviet military. Through Pakistan and Saudi Arabia, the CIA provided billions in support for arms and training and played an important role in helping the insurgents force the Soviets to withdraw (although it also inadvertently helped to create the Al Qaeda network that would plague the United States a decade later).[32]

Another major and more controversial operation at the time occurred in Nicaragua and involved creating the *contra* resistance force in an attempt to destabilize and overthrow the new Nicaraguan Sandinista regime. The *contra* covert war was eventually outlawed by Congress in the early 1980s. Nevertheless, the

Reagan administration circumvented the law by pursuing the *contra* operation through the NSC staff and relying on private operatives and groups.[33] The administration attempted to destabilize the country and overthrow the government. The U.S. "rollback" policy under DCI Casey predominantly consisted of a major covert operation devised by the CIA to develop, train, equip, and support a counterrevolutionary force of Nicaraguans, known as the contras, that grew to a 10,000–15,000-strong military force. These activities also included CIA—rather than *contra*—attacks on Nicaraguan oil installations and mining of Nicaraguan harbors; the secret channeling of military equipment to the contras from the Pentagon or cooperative third countries (such as Honduras and Panama); CIA preparation of a training manual for the contras that may have advocated assassination; and efforts to pressure Costa Rica (which was officially neutral) to support the creation of a southern front for the contras (such as the CIA staging phony Sandinista raids on the Costa Rican border).

The Reagan administration took other steps to expand CIA operations. First, the administration eased many restrictions on the conduct of intelligence operations within the United States.[34] In addition, the administration also tightened the security and secrecy system that had developed throughout the intelligence community and the government. It became much more difficult for the public to gain access to information under the Freedom of Information Act. Moreover, to pursue its covert operations, the Reagan administration resisted and circumvented congressional oversight of the intelligence community. It was such actions that triggered the Iran-contra affair and caused Reagan's final two years to be dominated by investigations of this scandal, along with concerns that the CIA was out of control.

Adjusting to the Post–Cold War and Post–9/11 Periods

The Cold War's end ushered in a set of challenges for the CIA and its covert action mission, which appeared much less central to U.S. foreign policy without the Cold War's context. According to Theodore Draper, "Of all the organizations that miss having the Soviet Union as an enemy, the CIA has undoubtedly been hit the hardest. The reason is that the CIA was specifically established in 1947 to struggle with the Soviet enemy. . . . But now the enemy has vanished. Its most dedicated American antagonist has been deprived of its mission. . . . [Now] the CIA wanders about in a wilderness of self-doubt and recrimination."[35] Recent years have not been much kinder, as the spectacular failures of September 11, 2001, and Iraq left the CIA reeling. One recent analysis concluded the CIA has "lost its place and standing in Washington," while a CIA veteran reacted to the 2004 intelligence reforms by saying, "The agency, as we know it, is gone."[36] Yet in late 2005, the CIA's central role in coordinating covert operations was confirmed with the strengthening of the National Clandestine Service, the new name for its directorate of operations. And after September 11, the agency's covert antiterror programs grew into the largest covert action program since the height of the Cold War.[37]

Prior to this recent expansion, however, as the CIA sought new missions in the post–Cold War context, its budget growth first slowed under George H. W. Bush and then began to decline under Bill Clinton. At the same time, challenges to CIA activities began. Congress attempted to enact tighter controls over covert action, but Bush vetoed the legislation in 1992. Not long after, Senator Daniel Patrick Moynihan (D-NY) sponsored legislation to eliminate the CIA entirely, ending covert action and placing the agency's intelligence analysis function in the State Department. Between 1990 and 2001, a spate of studies—some from Congress, some from special commissions, and some from policy think-tanks—all recommended reforms of the intelligence community.[38]

In the midst of this turmoil, the CIA continued some traditional covert operations, and added some new actions as well. For example, the agency applied its traditional instruments in the 1990s against Iraq and Kosovo. In Iraq, starting with a Bush (Sr.) finding that authorized efforts to destabilize the Iraqi economy in 1990 (after the Iran-Iraq War), the CIA engaged in a series of efforts to undermine Saddam Hussein, none of which was particularly effective. Under Bill Clinton, for example, the CIA supported the Iraqi National Congress, spending about $120 million seeking Hussein's assassination or overthrow. These operations collapsed when the resistance was infiltrated by Hussein's forces, although the United States committed itself to regime change in Iraq again in 1998. The initial campaign was an unmitigated disaster, however—"the greatest covert action debacle since Vietnam" in the words of two observers.[39] In Kosovo in 1999, the CIA launched a campaign against Serbia and Slobodan Milosevic that combined propaganda, destabilization, support of opposition groups, and other methods to undermine the regime.[40]

At the same time, the CIA took up a role in new areas as well, including drug trafficking, economic intelligence, and counterterrorism. On the drug war, the CIA began to cooperate with other agencies, including the FBI and the Drug Enforcement Agency, to break up drug rings. The CIA also increased its activities in the highly controversial arena of economic espionage, not only collecting information on trade practices but even attempting to steal trade secrets. Finally, with rising concerns about terrorism after the 1993 World Trade Center bombing, the CIA accelerated its counterterrorism operations as well. Osama bin Laden and theAl Qaeda network were especially important targets, and the CIA established a new counterterrorism center and a "bin Laden station" to oversee its efforts. Although some success occurred, the attacks in 1998 on U.S. embassies in Kenya and Tanzania, the 2000 bombing of the USS *Cole* in Yemen, and, of course, the September 11, 2001, attacks amply demonstrate the limits to the efforts.[41]

The attacks of 9/11 initiated a new season for the CIA and its covert operations mission. Just a few days after the attack, George W. Bush signed a presidential finding starting what has grown into the largest covert operation since the heydays of the Cold War, dwarfing even the decade-long Afghanistan operations of the 1980s. In addition to activities in advance and support of U.S. operations in Afghanistan and Iraq, the CIA began a host of interrelated programs to break up

terror cells, assassinate terrorists, capture and interrogate Al Qaeda suspects, gain access to and disrupt financial networks, eavesdrop, and a variety of other activities.[42] As Bob Woodward reported, "The gloves are off. The president has given the agency the green light to do whatever is necessary. Lethal operations that were unthinkable pre-September 11 are now underway."[43] The CIA budget was again increased, rising from about $27 billion in 1998 to over $44 billion in 2005. For the first time in a decade, the CIA began to expand its operations directorate as well, and the counterterrorism center at the agency more than doubled in size, becoming the center of covert actions against terrorism.[44]

At the same time, however, the CIA came under criticism for its failures to prevent the 9/11 attacks and then, later, for its role in the prewar Iraq intelligence fiasco. A number of investigations issued scathing reports of CIA failures. Additionally, as some of the covert actions become public—especially the CIA programs for assassination, capture and interrogation, rendition, and its secret prison system—heightened scrutiny was instigated. Hence, by 2006, with major intelligence reform weakening the CIA's role, sagging morale from the failures of the previous five years, and new challenges from the Defense Department for roles in covert operations, the future of CIA activities in this arena was far from certain.[45]

METHODS OF COVERT ACTION

In light of this brief overview, it is perhaps no surprise that when most people think of the CIA, they think of covert operations and "dirty tricks." Covert operations involve a variety of operations, where so-called dirty tricks and coercive force are most commonly practiced. According to an important NSC document from the Eisenhower administration, covert action included

> Propaganda, political action; economic warfare; escape and evasion and evacuation measures; subversion against hostile states or groups including assistance to underground movements, guerrillas and refugee liberation groups; support of indigenous and anticommunist elements in threatened countries of the free world; deception plans and operations; and all activities compatible with this directive necessary to accomplish the foregoing.[46]

Most observers lump such covert actions into four or five broad categories. According to Johnson, for example, covert action includes propaganda, political, economic, and paramilitary operations.[47]

Propaganda

Propaganda involves the use of information to influence the climate of opinion. Much of this activity is done overtly, through government statements, published information in the media and other outlets, television and radio broadcasts, and a

wide variety of other means. When such information is disseminated in a way that keeps the true sponsor secret, it becomes a covert action. By far the most common covert action, propaganda of a variety of kinds has been a staple of American covert policy since World War II.[48] The brief survey above includes a number of examples of propaganda ranging from so-called white propaganda to gray and black propaganda. White propaganda is overt, essentially truthful information disseminated through official government pronouncements, broadcasts, and other means. The activities of the U.S. Information Agency (until its dissolution in 1999), as well as Radio Liberty/Radio Free Europe are good examples. According to Godson, "Gray propaganda hides its sources from the uninitiated public, but not from sophisticated observers."[49] The information itself may range from essentially true to one-sided to false. Black propaganda occurs "when the source is false and well concealed, or when the information itself is false" or both.[50] Examples include forgery, rumor, disinformation and the like. According to Loch K. Johnson, "the CIA provides a flood of supportive but unattributed propaganda, distributed through its vase network of media 'assets' (paid agents): reporters newspaper and magazine editors, television producers—the whole range of personnel in the print and electronic media. . . . the extensive CIA propaganda capability produces a great tide of information flowing secretly from Washington into hundreds of hidden channels around the world."[51]

Political Activity

Usually in combination with propaganda, political activity involves more direct action to affect the political situation in a given country. Typically, such actions involve secret support provided to nationals, parties, or organizations of another country. For example, when the CIA provided covert assistance to political parties in Italy or France in the 1948 elections, anti-Allende parties in Chile in the 1960s, and anti-Milosevic factions in Yugoslavia in 1999, these were instances of political activity. According to Treverton, political activity might typically involve support for media, labor unions, and political parties; influencing elections; and support for individuals or other groups.[52] Such support may range from simple financial aid to more complex campaigns of support. At times, as one long-time analyst of the CIA has described, "the Covert Action Staff at CIA headquarters has resembled nothing less than a group of political campaign consultants, producing slick materials for favored foreign candidates."[53] Not only do propaganda and political action work together, but many major paramilitary operations of the kind already discussed began as political action.[54]

Economic Activity

A third category of covert action involves efforts to disrupt the economy of another country. Of the examples presented in the preceding summary, operations in Cuba and Chile provide good representations. In Cuba, the CIA engaged

in numerous activities to undermine the economy, including an abortive plan to contaminate Cuban sugar with chemicals, the sabotage of shipments of machinery and spare parts, and raids against railroads, oil and sugar refineries, and other factories.[55] In Chile, a variety of efforts were undertaken to destabilize the economy and create unrest to undermine the Allende regime. More recently, economic activities were central to the range of covert actions designed to bring pressure to bear on Slobodan Milosevic in Yugoslavia and currently play a key role in the extensive covert actions in the war on terrorism.

Paramilitary Operations

The most intrusive—and, paradoxically, high profile—type of covert action are extensive secret wars directed against hostile states (or other targets). According to John Prados,

> American secret wars have been carried out on almost every continent since . . . 1947. These covert operations have involved thousands of native fighters, significant numbers of American clandestine agents, and even regular United States military forces. United States involvement has run the gamut from advice to arms, from supplying full support for invasions of independent nations to secret bombing in support of clandestine military operations.[56]

The paramilitary campaigns in Guatemala, Cuba, Angola, Afghanistan, Nicaragua, and Iraq discussed earlier provide good examples and illustrate the range of activities involved in such operations, from full-scale wars to "little more than the clandestine transfer of a few weapons or of small amounts of training."[57] Also included in this category are assassinations, prohibited since the 1970s by executive order. However, in the wake of the 2001 terrorist attacks on New York and Washington, George W. Bush signed an intelligence order authorizing assassinations of terrorist leaders through such high-tech means as the use of the unmanned Predator drones equipped with Hellfire missiles.[58]

With respect to these categories, one last point bears mentioning. As the descriptions of Guatemala in the 1950s, Nicaragua in the 1980s, and the covert operations against terrorism in the early twenty-first century indicate, covert action typically involves a *campaign* of activities from these categories. At their most successful, such campaigns are carefully orchestrated and integrated into broader foreign policy plans and purposes.

The "Ladder of Escalation" for Covert Operations

According to Loch K. Johnson, covert actions such as those summarized in the preceding pages can be arrayed along a ladder of escalation as modest intrusions, high risk, and extreme categories (see Table 4-2). Covert actions all fall above the first "threshold" on the ladder dividing "routine intelligence operations" from

Table 4-2. Covert Action and the "Ladder of Escalation"

Extreme Options	Use of chemical-biological, other deadly agents
	Major secret wars
	Assassination plots
	Small scale coups d'état
	Major economic dislocation
	Environmental alterations
	Pinpointed retaliations against noncombatants
	Torture
	Hostage taking
	Major hostage rescue attempts
	Theft of sophisticated weapons or matériel
	Sophisticated arms supplies
High-Risk Options	Massive increases of funding in democracies
	Disinformation against democratic regimes
	Disinformation against autocracies
	Small-scale hostage rescue attempts
	Training of foreign military forces for war
	Limited arms supplies for offensive purposes
	Limited arms supplies for balancing purposes
	Economic disruption without loss of life
	Large increases of funding in democracies
	Truthful, contentious information in democracies
	Truthful, contentious information in autocracies
Modest Intrusions	Low-level funding of friendly groups
	Truthful, benign information in democracies
	Truthful, benign information in autocracies

Source: Adapted from Loch K. Johnson, "On Drawing a Bright Line for Covert Operations," *American Journal of International Law* 86 (April 1992), p. 286.

more intrusive actions.[59] For the purposes of this chapter, the ladder of escalation provides a convenient means to organize the methods of covert activity. With each step up the ladder, the activities become more risky and more likely to trigger a response. Actions on the highest end of the ladder are also the most controversial in terms of both domestic accountability and international law. As such, they must be carefully considered and tightly integrated into foreign policy tactics, strategies, and objectives. Because the options at the high end of the ladder increase in both risk and controversy, such methods demand greater accountability

DILEMMAS AND CONSIDERATIONS

We conclude this chapter with a few observations on the dilemmas posed by the methods of covert action, followed by a synthesis of guidelines for increasing

their legitimacy and effectiveness. First, and most broadly, use of and attitudes toward covert action are strongly shaped by the foreign policy ethos of the time, which is strongly influenced by the nature of threat. When perceptions of enemy threat are high, the demands of national security tend to prevail, resulting in the rise of intelligence activities, particularly covert operations. When threat perceptions decline, democratic considerations tend to rise, and the legitimacy of intelligence functions, especially covert operations, is often questioned.[60] This helps explain the major patterns in our historical overview: (1) During the Cold War years of high threat perceptions, acceptance of and latitude for covert action was greatest; (2) after the Vietnam War, lower threat perceptions prevailed and covert actions received more scrutiny; (3) the 9/11 attacks and the war on terrorism have so far resulted in a similar pattern, with national security demands—and thus support for covert action—ascendant in the immediate postattack period, whereas concerns for the methods and legitimacy of covert action growing after 2003 when the threat environment appeared less urgent. As Godson explains,

> The acceptance of covert action in the 1940s and 1950s, based on the perception of external threat, gave way, beginning in the 1960s and continuing on into the 1980s, to a quite different ethos. That new ethos, "exceptionalism," has over the course of its development wreaked havoc on American covert action capabilities. . . . Exceptionalism holds that covert action should not be engaged in unless there are grave and unusual circumstances.[61]

Within this context, both policy and accountability dilemmas exist.

Policy Dilemmas

With respect to policy dilemmas, as many observers have routinely noted, there are legal, moral, and practical dilemmas posed by the methods of covert action. Legally, covert action poses dilemmas because "many covert operations, if carried out by different persons and under other circumstances, would be plainly and seriously criminal," as Berkowitz and Goodman have characterized it.[62] This is true in terms of national laws, but there are also international legal concerns posed by the methods we have discussed, beginning with their implications for norms of sovereignty.[63] As well, morally, dilemmas arise from the dirty tricks and coercive nature of many of the methods. Practically the dilemmas stem from the costs, trade-offs, and long-term implications of covert actions. For example, resort to propaganda bears with it the potential for blowback, whereby disinformation intended to influence a foreign target is recycled into the American media, thereby impacting the U.S. public.

Similarly, the excesses of CIA covert operations often damaged the reputation of the U.S. government and its foreign policy. In Iran, for example, the U.S. government overthrew a nationalist leader, installed the shah on the throne, and backed his ruthless dictatorship for over twenty-five years. This knowledge

should allow Americans to better understand the hatred that so many Iranians felt toward the U.S. government and why the United States was portrayed by many Iranians as the Great Satan since the 1970s, especially under Ayatollah Khomeini. CIA excess has also bred mistrust among U.S. allies, whose secrets have been compromised and whose involvement risks considerable political embarrassment. Finally, it has bred distrust and cynicism among the American public about their own government.[64]

Accountability Dilemmas

In terms of accountability dilemmas, the crux of the matter concerns the extensive secrecy and deniability demanded by covert action, on one hand, and the demands of democracy on the other. Since the erosion of the Cold War consensus, serious concerns about the potential for excess has driven repeated searches for appropriate and effective oversight measures whereby the activities of the intelligence community can be reconciled with the demands of democracy. In the wake of the controversies of the 1970s, the Iran-*contra* episode, and the more recent failures and excesses concerning the war on terror, adequate and appropriate oversight remains a concern.[65] Congress asserted itself in the 1970s after the first wave of revelations, establishing new intelligence committees and oversight procedures, but problems continued. On one hand, democracy requires that governmental agencies be held accountable to elected leaders and the public. The demands of national security, on the other hand, often require a quick and efficient foreign policy response. A premium is placed on the independence and secrecy of governmental operations to keep the enemy at bay. The use of all available means to protect and further national security is often considered a necessity in a world where morality is seen to have little relevance. Covert action, by its nature, therefore generates a fundamental tension in a democratic society.

Guidelines for Legitimacy and Effectiveness

Given the methods and controversies of covert action, it is no surprise that many policy makers, practitioners, observers, and analysts have expressed concern for guidelines for employing such options. Table 4-3 presents a select list of such concerns, synthesized from the work of leading analysts.[66] As the table indicates, we organize them into three categories: relevance, coherence, and consequences. For relevance, the guidelines urge consideration of the desirability and applicability of covert methods. In particular, they recommend careful weighing of such issues as the need and possibility for deniability, the nature of the target, the relevance of other options, and perhaps most significant, the unsuitability of covert action as a way to take action in the face of pressure to do something when other options appear impossible. Those guidelines related to coherence build on this last point and emphasize, first, the need to embed covert action into a broader foreign policy strategy with explicit goals and objectives (including assessment

Table 4-3. Guidelines for Covert Action Legitimacy and Effectiveness

Relevance	Make sure deniability is necessary and possible
	Consider the nature of the target
	Carefully consider other options, including diplomacy, first
	Consider proportional response and opt for actions at the lowest end of the "ladder of escalation"
	Do not resort to covert action for crisis resolution
	Do not resort to covert action as a last resort in the absence of other viable policy options
	Do not resort to covert action to rescue a failed policy
Coherence	Embed covert action in a strategy that makes geopolitical sense
	Tie covert action to specific goals and carefully defined objectives
	Ensure that covert action is in harmony with publicly stated policy objectives
	Evaluate covert action options through the full interagency process, including consultation with intelligence analysts, not just covert action specialists
	Never violate U.S. laws, including reporting requirements
Consequences	Consider blowback possibilities and consequences
	Consider consequences of the covert action becomes public, including the possibility of embarrassment and the impact on reputation
	Consider consequences if first step in covert action is unsuccessful
	Consider what signal the covert action will send, to whom, and with what result

of the nature of the threat) and, second, to ensure that the covert options are carefully vetted through the interagency process and consistent with U.S. laws (including procedural rules for reporting, oversight, and the like). The guidelines related to consequences urge careful consideration of the short- and long-term consequences of the covert action, including key questions about the implications of exposure, failure, and blowback. As Godson suggests, a key question that must be asked is "what if—or more likely, when—it becomes public."[67]

CONCLUSION

Since World War II, the U.S. has engaged in a wide variety of covert actions all over the globe. During the Cold War, such activities were widely accepted and justified as a necessary part of the intense ideological and geopolitical struggle with the Soviet Union. After the Vietnam War and the revelation of the extent and consequences of covert actions in highly controversial settings such as Cuba, Vietnam, and Chile, to name a few, covert action came under increased scrutiny as Congress in particular sought to exercise greater oversight. For many, the

gung-ho enthusiasm of the Cold War gave way to a reluctant exceptionalism that has generated considerable tension since the 1970s. The emergence of terrorism as a central concern in the twenty-first century injected new life into covert action as a foreign policy tool, especially since the shady world of terrorism would seem to be an especially rich target for covert action. The demands of such a "war" would seem to ensure that policy makers will continue to reach for covert action methods of the kinds reviewed here—and new ones to contend with the new environment—to address threats and achieve objectives.

NOTES

1. David F. Rudgers, "The Origins of Covert Action," *Journal of Contemporary History* 35, no. 2 (April 2000), p. 252.

2. Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence in the Information Age* (New Haven, CT: Yale University Press, 2000).

3. Quoted in John Ranelagh, *The Agency: The Rise and Decline of the CIA* (New York: Touchstone, 1987), p. 134.

4. Loch K. Johnson, "Covert Action and Accountability: Decision-Making for America's Secret Foreign Policy," *International Studies Quarterly* 33 (March 1989), p. 82.

5. Executive Order 12333, *United States Intelligence Activities*, December 4, 1981.

6. Intelligence Authorization Act of 1991, Public Law 102-88, 105 Stat, 429 (1991), Section 503 [c][4][e].

7. William J. Daugherty, *Executive Secrets: Covert Action and the Presidency* (Lexington: University Press of Kentucky, 2004), p. 12.

8. Berkowitz and Goodman, *Best Truth*, pp. 129–30. See also Daugherty, *Executive Secrets*, p. 16.

9. Daugherty, *Executive Secrets*, p. 13.

10. Johnson, "Covert Action and Accountability," p. 84.

11. See Rhodri Jeffrey-Jones, *CIA and American Democracy*, 3rd ed. (New Haven, CT: Yale University Press, 2003); Loch K. Johnson, *America's Secret Power* (New York: Oxford University Press, 1991); Jonathan Kwitny, *Endless Enemies: The Making of an Unfriendly World* (New York: Penguin, 1984); John Prados, *Presidents' Secret Wars: CIA and Pentagon Operations Since World War II* (New York: William Morrow, 1986); Ranelagh, *The Agency*; U.S. Senate, *Alleged Assassination Plots Involving Foreign Leaders*, Congressional Report, 94th Congress, 1st sess. (November 18, 1975); and U.S. Congress, Senate, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, Books 1–6, Congressional Report, 94th Congress, 2nd sess. (April 14, 1976). See also Loch K. Johnson, "The Contemporary Presidency: Presidents, Lawmakers, and Spies: Intelligence Accountability in the United States," *Presidential Studies Quarterly* 34 (December 2004), pp. 828–37 for a similar set of stages in the evolution of covert activities.

12. For example, see Rudgers, "The Origins of Covert Action," pp. 259–61.

13. In interpreting the meaning of the act's phrase, the CIA's first general counsel, Lawrence Houston, concluded that "taken out of context and without knowledge of [the act's] history, these Sections could bear almost unlimited interpretation. In our opinion,

however, either [propaganda or commando type] activity would be an unwarranted extension of the functions authorized" by the act. "We do not believe that there was any thought in the minds of Congress that the Central Intelligence Agency under this authority would take positive action for subversion and sabotage." Any such missions would necessitate going to Congress "for authority and funds." Such authority eventually was provided by passage of the Central Intelligence Act of 1949 (Jay Peterzell, "Legal and Constitutional Authority for Covert Operation," *First Principles* 10 [Spring 1985], pp. 1–3). See also Jeffrey-Jones, *CIA and American Democracy*, chapter 3.

14. Johnson, "Covert Action and Accountability," p. 87.

15. See Peter Grose, *Gentleman Spy: The Life of Allen Dulles* (Boston: Houghton Mifflin, 1995); Jacob Heilbrunn, "The Old Boy at War," *New Republic,* March 27, 1995, pp. 32–37.

16. David Barrett, *The CIA and Congress: The Untold Story from Truman to Kennedy* (Lawrence: University of Kansas Press, 2005); see also Harry Howe Ransom, "The Politicization of Intelligence," in Steven J. Cimbala, ed., *Intelligence and Intelligence Policy in a Democratic Society* (Dobbs Ferry, NY: Transnational, 1987), pp. 25–46.

17. Senate, *Final Report*, p. 9.

18. Harry Howe Ransom, "Strategic Intelligence and Intermestic Politics," in *Perspectives on American Foreign Policy: Selected Readings,* eds. Charles W. Kegley Jr. and Eugene R. Wittkopf (New York: St. Martin's, 1983), p. 303.

19. U.S. Congress, Senate*, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Foreign and Military Intelligence*, Book I, Congressional Report, 94th Congress, 2nd sess. (April 14, 1976), p. 445.

20. Jeffrey-Jones, *CIA and American Democracy*, p. 51.

21. See James A. Bill, *The Eagle and the Lion: The Tragedy of American-Iranian Relations* (New Haven, CT: Yale University Press, 1988), and Jonathan Kwitny, *Endless Enemies: The Making of an Unfriendly World* (New York: Penguin, 1984).

22. See Richard H. Immerman, *The CIA in Guatemala: The Foreign Policy of Intervention* (Austin: University of Texas Press, 1982), and Stephen Schlesinger and Stephen Kinzer, *Bitter Fruit: The Untold Story of the American Coup in Guatemala* (New York: Doubleday, 1982).

23. See Madelaine G. Kalb, *The Congo Cables: The Cold War in Africa from Eisenhower to Kennedy* (New York: Macmillan, 1981).

24. U.S. Department of State, *Foreign Relations of the United States* (1950), vol. 2, p. 607.

25. Joseph Albright and Marcia Kunstel, "CIA Tip Led to '62 Arrest of Mandela: Ex-Official Tells of U.S. 'Coup' to Aid S. Africa," *Atlanta Constitution*, June 10, 1990, p. A14.

26. See Peter Wyden, *Bay of Pigs: The Untold Story* (London: Jonathan Cape, 1979).

27. Jeffrey-Jones, *CIA and American Democracy*, p. 132.

28. See John Stockwell, *In Search of Enemies: A CIA Story* (New York: Norton, 1978).

29. Loch K. Johnson, "Accountability and America's Secret Foreign Policy: Keeping a Legislative Eye on the Central Intelligence Agency," *Foreign Policy Analysis* (March 2005), pp. 99–120; Loch K. Johnson, "Covert Action and Accountability," pp. 81–109.

30. See Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001* (New York: Penguin, 2004).

31. Philip Taubman, "Casey and His CIA on the Rebound," *New York Times Magazine*m January 16, 1983, p. 21.

32. On the Afghanistan operation, see Coll, *Ghost Wars*; George Crile, *Charlie Wilson's War* (New York: Atlantic Monthly Press, 2003); and James M. Scott, *Deciding to Intervene: The Reagan Doctrine and American Foreign Policy* (Durham, NC: Duke University Press, 1996).

33. On the Nicaragua operation, see Robert Kagan, *A Twilight Struggle: American Power and Nicaragua, 1977–1990* (New York: Free Press, 1996), and Scott, *Deciding to Intervene*.

34. See, for example, Duncan L. Clarke and Edward L. Neveleff, "Secrecy, Foreign Intelligence, and Civil Liberties: Has the Pendulum Swung Too Far?" *Political Science Quarterly* 99 (Fall 1984), pp. 493–513, and Stansfield Turner and George Thibault, "Intelligence: The Right Rules," *Foreign Policy* 48 (Fall 1982), pp. 122–38.

35. Theodore Draper, "Is the CIA Necessary?" *New York Review of Books*, August 14, 1997, p. 18.

36. James Risen, *State of War: The Secret History of the CIA and the Bush Administration* (New York: Free Press, 2006); Siobhan Gorman, "New Intelligence Director Shakes up Hierarchy," available at www.govexec.com/dailyfed/0505/050905nj1.htm.

37. Siobhan Gorman, "New Clandestine Service to Coordinate U.S. Spying," *Baltimore Sun*, October 14, 2005, p. 2A.

38. See, for example, U.S. House of Representatives, Permanent Select Committee on Intelligence, *Intelligence Community in the 21st Century* (1996); Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (1996); and Council on Foreign Relations, *Making Intelligence Smarter: The Future of U.S. Intelligence*, Report of an Independent Task Force for the Council on Foreign Relations (1996).

39. Bruce D. Berkowitz and Allan E. Goodman, "The Logic of Covert Action," *National Interest* 51 (Spring 1998), p. 44.

40. See, for example, Roy Godson, *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence* (New Brunswick, NJ: Transaction, 2000); Loch K. Johnson, *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security* (New York: New York University Press, 2000); James Risen, "The Clinton Administration's See-No-Evil CIA," *New York Times,* September 10, 2000, p. 5.

41. On these activities, see Robert Baer, *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terror* (New York: Arrow Books, 2002); Berkowitz and Goodman, *Best Truth*; Richard Clarke, *Against All Enemies* (New York: Free Press, 2004); Godson, *Dirty Tricks or Trump Cards*; Johnson, *Bombs, Bugs, Drugs, and Thugs*; and Timothy Naftali, *Blind Spot: The Secret History of American Counterterrorism* (New York: Basic Books, 2005).

42. See, for example, Clarke, *Against All Enemies*; Risen, *State of War*; Dana Priest, "Covert CIA Program Withstands New Furor," *Washington Post*, December 30, 2005, p. A1; Gary Schroen, *First In: An Insider's Account of How the CIA Spearheaded the War on Terror in Afghanistan* (New York: Presidio Press, 2005).

43. Bob Woodward, "CIA Told to Do 'Whatever Necessary' to Kill Bin Laden," *Washington Post*, October 21, 2001, p. A1.

44. Walter Pincus, "Intelligence Shakeup Would Boost CIA," *Washington Post*, November 8, 2001, p. A1.

45. See the 9/11 Commission Report, U.S. Senate, Select Committee on Intelligence, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq* (2004); Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction in Iraq, *Report of the President* (March 3, 2005); and Risen, *State of War*.

46. Jeffrey-Jones, *CIA and American Democracy*, p. 83.

47. Roy Godson discusses propaganda, political action, paramilitary activity, and intelligence assistance in *Dirty Tricks or Trump Card*, and Daugherty discusses propaganda, political action, paramilitary operations, and information warfare in *Executive Secrets*. Lowenthal uses a five-part scheme of propaganda, political activity, economic activity, coups, and paramilitary operations in *Intelligence: From Secrets to Policy* (Washington, DC: Congressional Quarterly Press, 2006). Treverton, by contrast, only discusses propaganda, political action, and paramilitary operation in *Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, 1987).

48. See, for example, Treverton, *Covert Action*; Johnson, "Covert Action and Accountability," p. 84.

49. Godson, *Dirty Tricks or Trump Cards*, p. 152.

50. Ibid., p. 154.

51. Johnson, "Covert Action and Accountability," p. 84.

52. Treverton, *Covert Action*, pp. 17–25.

53. Johnson, "Covert Action and Accountability," p. 85.

54. For example, Johnson, "Covert Action and Accountability," p. 85; Treverton, *Covert Action*, p. 17.

55. Prados, *Presidents' Secret Wars*, p. 212.

56. Ibid., p. 15.

57. Treverton, *Covert Action*, p. 26.

58. Bob Woodward, "CIA told to do 'whatever necessary,'" p. A1.

59. Loch K. Johnson, "On Drawing a Bright Line for Covert Operations," *American Journal of International Law* 86 (April 1992), pp. 284–309.

60. Ransom, "Strategic Intelligence and Intermestic Politics," pp. 299–319.

61. Godson, *Dirty Tricks or Trump Cards*, p. 64.

62. Berkowitz and Goodman, "The Logic of Covert Action," p. 38.

63. A good discussion is Johnson, "Drawing a Bright Line."

64. See Anthony Lake, "Lying Around Washington," *Foreign Policy* 2 (Spring 1971), pp. 91–113.

65. On this matter, see Frank Smist, *Congress Oversees the Intelligence Community, 1947–1994* (Knoxville: University of Tennessee Press, 1994); Loch K. Johnson, "Acountability and America's Secret Foreign Policy"; Johnson, *America's Secret Power*; Jeffrey-Jones, *CIA and American Democracy*, among others.

66. These guidelines are synthesized from Johnson, "Drawing a Bright Line"; Berkowitz and Goodman, "The Logic of Covert Action"; Lowenthal, *Intelligence*; Daugherty, *Executive Secrets*, and Godson, *Dirty Tricks or Trump Cards.*

67. Godson, *Dirty Tricks or Trump Cards*, p. 216.

5

COVERT ACTION

An Appraisal of the Effects of Secret Propaganda

MICHAEL A. TURNER

SECRET PROPAGANDA IS AN ESSENTIAL PART OF America's covert action capabilities. The 1991 Intelligence Authorization Act, which currently governs the covert action reporting process, defines covert action as an "activity or activities of the U.S. Government to influence political, economic, or military conditions abroad, where it is intended that the [U.S.] role will not be apparent or acknowledged publicly." Implicit in this definition is the fact that covert actions involve interference in the domestic affairs of other states or the internal workings of nonstate groups. This invariably makes such operations highly problematic from operational and ethical viewpoints. The generally accepted standard today, first embodied in Executive Order 12036 of 1978 and reaffirmed in various other orders since then, is that covert actions are to be employed only when essential to the national security of the United States and as a last resort. Secret propaganda, a form of covert action, has historically been excluded from this formulation despite its dubious benefits.

COVERT ACTION TYPES

The U.S. government engages in three categories of covert actions, each of which contains a bewildering range of activities. Political and economic actions are the most obvious and historically the most notorious, in that they involve instigating changes in governments, leadership, or social conditions. For example, the covert operations to prevent Salvador Allende from winning Chile's presidency in 1970 and then to oust him from office in 1973 fell into this category. This category of actions also includes assistance to political parties and labor

unions as well as political assassination attempts—of Cuba's Fidel Castro or the Congo's Patrice Lumumba, for example. It says a good deal about their controversial nature that the Chilean operations and the attempts against Castro served as catalysts for the public investigations of U.S. intelligence in general and the Central Intelligence Agency (CIA) in particular during the mid-1970s.

Political and economic actions also include covert support to paramilitary groups and insurgents. According to press reports, the United States, for example, gave military assistance to moderate Afghan dissident groups during the Carter administration in the late 1970s and, following the Soviet invasion in 1979, to Afghan rebels, some of whom were Islamic extremists who later turned their insurgent capabilities against the United States.[1]

The second category of covert actions is paramilitary activity, which often involves the use of CIA's own paramilitary forces or joint arrangements with the U.S. military for combat operations and activities like sabotage. Most paramilitary (as well as political and economic) actions make liberal use of the third type of covert action—propaganda—as the lead or supplemental covert activity. *Propaganda* is defined as the dissemination of information intended to manipulate perceptions in support of one's cause or to damage an adversary.

From the start, when the 1947 National Security Act set up the CIA and later legislation gave the agency responsibility for managing America's covert actions, there has been a symbiosis among the three types of covert operations. By 1953, the CIA's Office of Secret Operations had merged with the Office of Policy Coordination (OPC), the government's covert action arm, to set up CIA's Directorate of Plans. According to the *Los Angeles Times*, this directorate established a massive propaganda machine, with thousands of employees who were adept at not only placing press and radio stories but also in simultaneously carrying out such covert acts as engaging with labor unions, applying economic pressure, offering direct money payments, and waging political and cultural warfare—all to prevent European countries from falling to the communists. The *Los Angeles Times* also asserts that the congressional investigations in the mid-1970s revealed that by then CIA owned or subsidized at various times more than fifty newspapers, news services, radio stations, periodicals, and other communication facilities, most of them abroad. In some cases, these assets were used for propaganda purposes; in other instances, they served as covers for other operations. In any event, paid CIA agents infiltrated a dozen foreign news organizations, and at least twenty-two American news outlets employed journalists working for the CIA. Nearly a dozen U.S. publishing houses printed more than a thousand books that had been produced or subsidized by the CIA.[2]

Of the three types of covert actions, propaganda is an integral part of the government's influence operations. The most overt of these operations, public diplomacy, seeks to explain government policy and project soft power without attempting to hide government sponsorship. Soon after the terrorist attacks of September 11, 2001, the U.S. government began a public diplomacy effort, characterized by fits and starts, that has focused on three strategic imperatives. First,

the United States must offer a positive vision of hope and opportunity to people around the world, rooted in America's commitment to freedom. Second, the United States must isolate and marginalize violent extremists and undermine their efforts at terror. Third, the United States must foster a sense of common interests and common values between Americans and people of different countries, cultures, and faiths.[3]

Strategic influence operations, the second type of influence venture, are generally the domain of the U.S. military and attempt to alter attitudes and behaviors in favor of policy stands the U.S. government favors. Winning the hearts and minds of foreign populations is always a tricky proposition, but the *Quadrennial Defense Review Report* of 2006 says that victory in the war on terror depends on strategic communication.[4] Such operations may include information warfare, which is quickly becoming an important part of America's strategic posture.

Secret propaganda, the last of the three types of influence operations, may incorporate aspects of the previous two, in addition to psychological warfare operations. Though conceptually discrete, the three categories of influence operations overlap to such an extent that the best and most effective operation is one that employs the resources of all three and intermixes the capabilities in strategically significant ways.

SECRET PROPAGANDA

Because propaganda is often built around incomplete or false news stories in an effort to alter perceptions and elicit conditioned responses, its effectiveness often depends on such factors as the way statements are presented, the timing of the story's release, and the path it takes to get it into the media outlets. Experts agree that secret propaganda has three intended effects—mobilizing the target audience toward an intended objective, achieving concealment or surprise, or protecting legitimacy. Secret propaganda that seeks to mobilize does so either to persuade the target to commit itself in support of a cause or provide the illusion that old and new causes are compatible. An example of secret propaganda intended to mobilize is the British efforts prior to the onset of World War II to rally Americans to support the British cause. Another example is the effort by American senior military officers just prior to the 1968 Tet Offensive in Vietnam possibly to falsify Viet Cong order-of-battle figures and underreport North Vietnamese infiltrations of South Vietnam, all intended to strengthen the president's hand and convince the country and ultimately the North Vietnamese of America's determination to stay the course.

Secret propaganda to achieve surprise or to conceal plans usually occurs in wartime. Examples are the propaganda that accompanied the American interventions in the first Gulf War in 1991 and also just prior to the Iraq war in 2003, Soviet deception over the installations of the missiles in Cuba in 1962, and myriad efforts by various governments to mask weakness through a show of strength.

Secret propaganda to achieve, maintain, or restore legitimacy typically occur prior to, during, or just after military operations and are usually defensive in nature. Soviet interventions in Hungary, Suez, Czechoslovakia, Afghanistan, and Poland were accompanied by deceptions to protect legitimacy. The United States also engaged in secret propaganda to establish and defend the legitimacy of the Bay of Pigs operation in 1961. Propaganda to protect legitimacy also includes attempts to shift the blame for fiascoes, as did the Soviets after they shot down Korean Air flight 007 in 1983.

Today, numerous U.S. agencies, including the Department of Defense, engage in propaganda activities, but under U.S. law, propaganda is part of the covert action repertoire of the CIA. Propaganda activities range from overt (or white) propaganda—broadcasting news about the United States by Voice of America (VOA), for example—to black propaganda, which is spreading disinformation. Gray propaganda falls somewhere in between and includes broadcast activities intended to cast the United States in a positive light.

White Propaganda

White propaganda is the overt dissemination of factual but often biased information for strategic objectives. The activities of the U.S. Information Agency (USIA) during the Cold War, for example, were in the category of white propaganda, for that agency openly disseminated the U.S. policy line through libraries, cultural exchanges, publications, and media outlets. Although the USIA was disbanded in 1999, the U.S. government today floods the Iraqi and Afghan airwaves and print media with good news of schools opened after the U.S. military refurbishment, water systems repaired, or terrorist leaders captured—all truthful reports that essentially leave out items that may not be complimentary to U.S. interests.

Gray Propaganda

Gray propaganda, the second category, is the covert and unacknowledged dissemination of the official policy lines. Paying a journalist in a target country to write favorable reports about the United States, for example, would fit in this category. So would the surreptitious placement of favorable news items in foreign media outlets, as was the case for the past several years with the Pentagon's secret operations to provide a positive spin to America's efforts in Iraq. According to press reports, the Defense Department has secretly operated radio stations and newspapers in Iraq, placed editorials in Iraqi newspapers and websites, offered TV stations money to run unattributed segments, and contracted with writers of newspaper opinion pieces.[5] Furthermore, Pentagon contractors may have paid Iraqi Islamic religious leaders to offer propaganda advice and print positive articles about the American mission.[6]

This kind of unattributed propaganda has a long pedigree. At the onset of the Cold War, the U.S. government began employing propaganda as an instrument of its foreign policy, intended to "expose the fallacies of communism," warn of its dangers, strengthen Western-oriented regimes, increase awareness of the Soviet threat, and build greater willingness to cooperate with the West.[7] In June 1949, the CIA established the National Committee for a Free Europe to provide cover for a psychological warfare program that included radio propaganda to Eastern Europe. In July, Radio Free Europe (RFE) began broadcasting prodemocracy, anticommunist messages to Poland, Czechoslovakia, Hungary, Romania, and Bulgaria. It also beamed talks by exiles, personal messages, replies to mail from listeners, names of communist secret agents and informers, news items embarrassing the communist regimes, and American popular music banned in Eastern Europe. The CIA also founded RFE's sister station, Radio Liberty (RL), which broadcast similar messages to the Soviet Union in both Russian and the languages of the non-Russian peoples.[8]

The genius of these propaganda efforts was that far from lauding American popular culture or the Western way of life, they focused on issues closest to their listening publics, such as agricultural collectivization, the persecution of religion, the suppression of culture, party purges, and the like.[9]

Some American critics of the stations in the 1970s tried to shut them down, claiming that they were relics of the Cold War and served no useful purpose other than to goad the Soviet Union and its puppet regimes in Eastern Europe. This attempt failed, but the management of RFE/RL eventually was transferred from the CIA to an independent agency. RFE and RL were officially closed down on November 28, 2003, as a cost-saving measure.

One of the CIA's more daring and effective Cold War secret propaganda actions was the establishment of the Congress for Cultural Freedom in 1950. Initiated as a conference of intellectuals in West Berlin in June 1950, the congress published literary and political journals and hosted dozens of conferences bringing together some of the most eminent Western thinkers. Its purpose was to demonstrate that communism, despite its rhetoric, was an enemy of art and thought. By doing so, it sought to negate communism's appeal among artists and intellectuals and at the same time, undermine the communist claim to moral superiority. The CIA's sponsorship of the Congress for Cultural Freedom became publicly known in 1967, effectively ending the operation.[10]

The CIA undertook a similar propaganda venture against Fidel Castro beginning in 1960 as part of a larger covert operation against Cuba. Radio Swan carried programs taped in CIA radio stations in Miami, consisting of news analysis, entertainment, and anti-Castro speeches by Cuban exiles. The CIA also bought time in Caribbean stations for anti-Castro programming. Such programming continued well into the 1970s, stopping only after the congressional investigations of U.S. intelligence activities. Nonetheless, President Ronald Reagan announced plans on September 23, 1981, to revive a radio station to transmit

news reports to Cuba. Despite controversy and occasional attempts to disband the station, Radio Marti continues its broadcasts as part of the VOA.[11]

More recently, the United States engaged in psychological operations against Iraqi dictator Saddam Hussein during the first Gulf War in 1990–91 by inciting the Kurds, Shias, and other Iraqis to rise up against the regime. Press reports say that in addition to dropping leaflets over urban areas, messages were broadcast over two "black" radio stations, the Voice of Free Iraq and Radio Free Iraq, both of which were operated by the CIA. Once the ground war began in 1991, the Voice of Free Iraq stepped up its calls for an uprising by suggesting that Saddam Hussein was preparing to flee the country. Although these insurrections failed to materialize in 1991, America's propaganda promises paved the way for rebellions in 1995 that were brutally crushed by Iraq's dictator.[12]

Black Propaganda

Black propaganda, the purposeful manipulation of the perceptions of a target audience through the use of disinformation or deception, constitutes the third type of propaganda that the United States employs as part of its covert action arsenal. This general category, although used less frequently than the other two types, requires particular specificity to either direct the target into specific types of behaviors or alter attitudes of target audiences to forestall actions detrimental to U.S. interests. Black propaganda may employ white and gray propaganda to fulfill its goals, but its distinguishing characteristic is the nature of its content—information is either exaggerated or false. Given the nature of information technology today, black propaganda may involve spreading disinformation into government or terrorist computer networks.[13] As such, black propaganda more often than not is part of a broader covert action plan.

Black propaganda has been a potent instrument in CIA's arsenal since its inception. Beginning at the onset of the Cold War, the CIA infiltrated Western literature into the totalitarian regimes of the eastern bloc; sponsored anticommunist books written by Soviet and eastern bloc defectors as well as by American scholars; and developed media proprietaries abroad, including a secret propaganda printing plant in West Germany and various press outlets, such as the West German *Der Monat*, the British *Encounter*, and the Italian *Daily American*.[14]

In the campaign to prevent the Italian communists from coming to power in 1948, the CIA's psychological operatives inspired stories in the Italian press and letters from Italian Americans to their relatives in Italy. Funds were handed to Christian Democrats, in part for pamphlets, posters, and other paraphernalia of election campaigns. Publication of the Zorin Plan in *Tempo*, possibly a CIA disinformation story outlining Soviet plans for repressing Italy after the victory of the Italian communists, undoubtedly helped divert voters to the Italian socialists or the right-of-center Christian Democrats instead.[15]

In Guatemala in 1954, CIA engaged in secret propaganda by broadcasting the Voice of Liberation, a dissident station claiming to be based somewhere in the

Guatemalan countryside. The station broadcast the lie that a revolution was under way and an inflated number of troops were marching toward the capital—all calculated to encourage others to rally around the small cadre of CIA-backed insurgents and intimidate president Jacobo Arbenz Guzmán and his supporters into believing that they faced a superior force. This deception ultimately persuaded President Arbenz to flee the country.[16]

The CIA's attempts against Chile's Marxist politician Salvador Allende also involved propaganda in support of a wider covert operation. Much of this propaganda campaign involved discrediting Allende. The CIA spent $3 million in 1964 and another $3 million in 1972 to blacken his name. Between 1963 and 1973, when Allende was ousted by CIA-backed Chilean military officers, the agency spent $12 million on propaganda, employing extensive use of the press, radio, films, pamphlets, posters, leaflets, direct mailings, paper streamers, and wall painting.

On August 25, 1986, the *Wall Street Journal* ran a story that the United States was contemplating military or covert action against Libya and that internal opposition to Libyan leader Muammar Qaddafi was growing. The report in the American newspaper was actually blowback from a U.S. deception operation abroad, designed to create alarm in Libya and possibly precipitate Qaddafi's overthrow by Libyans.

The Soviets also were adept at black propaganda. In 1983 Moscow began a deception operation, first initiated in the Indian daily *Patriot*, designed to attribute blame for the AIDS epidemic to the United States by spreading the false story that the virus had been brought into existence by genetic engineering experiments conducted at Fort Dietrich, Maryland—allegedly to develop new biological weapons. Moscow then spread the story to Africa, South America, and Europe by advertising the investigations of a Soviet biochemist who supposedly had verified the link. The Soviet government acknowledged the disinformation campaign in 1989 and apologized for it, but to this day some extremist Americans and a substantial portion of Africa's population still hold to the fiction that the United States developed the HIV virus for use in the third world.

APPRAISING EFFECTS

Much of the U.S. government's information machinery, including the USIA and most covert action programs, were dismantled after the Cold War. The Department of Defense created an office soon after the 9/11 attacks to provide news items, both true and false, to foreign news organizations, but the office was quickly shut down after the plan became public and the effort was criticized as damaging U.S. credibility abroad.

Five years after 9/11, however, both the Pentagon and the CIA have undertaken a secret propaganda war to counter the insurgencies in Iraq and Afghanistan. The Pentagon has taken the lead in this effort and, together with CIA's

propaganda efforts, has been outsourcing its information campaigns to such contractors as Science Applications International, SyColeman, and the Lincoln Group.[17] For example, these firms have obtained contracts for "media approach planning" on behalf of the Joint Psychological Operations Support Element within the U.S. Special Operations Command.[18] Moreover, an intelligence expert asserts that half of the CIA's efforts have been outsourced to private contractors, which worries many people because these contractors are not subject to the kinds of controls or oversight that CIA employees experience.[19]

On balance, U.S. propaganda activities have had a mixed record. At the operational level, secret propaganda operations are effective (i.e., they succeed) under three conditions: the extent to which (1) their presentation attracts the intended target's attention and holds interest; (2) the effort does not alert the target to its presence; and (3) the target acts in the manner intended. All these factors aligned perfectly in the 1947 propaganda operation to keep the communists from electoral victory in Italy, which cost only about $10 million and resulted in the victory of pro-Western (and anticommunist) Christian Democrats. Logically then, secret propaganda fails if the target takes no notice of the presentation, notices but judges it to be irrelevant, misconstrues its intended meaning, detects the method of deception, or does not behave in the manner intended.

The effectiveness of secret propaganda operations also depends on the degree to which they remain secret. Once they become known, their effectiveness drops precipitously, and in many cases they become either an embarrassment to the government or result in negative and other unintended consequences. For example, in late September 1986, the deceptive nature of the Libyan operation was revealed in the press, and the Reagan administration was criticized for deceiving Americans as well as other publics. A similar result occurred when the *Washington Post* revealed that the U.S. military was planting positive stories in Iraq after the onset of the war in 2003.

On a broader level, secret propaganda can have positive as well as negative consequences. Whether the former outweighs the latter is unclear, but in either case, the legitimacy of secret propaganda appears to rest on the existence of a broad consensus about the country's foreign policy objectives and the means of achieving them. On the positive side, secret propaganda efforts like RFE and RL, whose existence remained unattributed well into the 1980s, benefited from broad consensus about the necessity of opposing the Soviet Union by employing methods short of nuclear war. These radio operations became well known and respected among their listeners. Some Polish leaders, for example, later asserted that the stations played an important role in bringing down at least three Polish Communist Party leaders and were instrumental in sustaining the Solidarity trade union in Poland when it was forced underground by martial law in 1981. During Romanian strongman Nicolae Ceausescu's time, RFE was Romania's most popular source of news. After the end of the Cold War, RFE/RL journalists visiting their target countries were greeted as heroes. Another successful propaganda effort was the CIA's effective campaign in the late 1970s to counter the Soviet propaganda

campaign against the U.S. deployment of the neutron bomb in Europe by comparing the bomb to the similarly dangerous Soviet SS-20 missile.

The propaganda effort to foment discontent within the Iraqi population in 1990–91 fell far short of sparking a popular uprising, primarily because of the pervasive internal security Saddam Hussein maintained, but these measures encouraged and gave false hope to the Kurds and the Shias subsequently to launch rebellions. In March 1995, Kurdish guerrillas trained by CIA launched raids against the Saddam Hussein regime, hoping to spark local insurrections, generate defections from government forces, and persuade Saddam that his army would not fight for him. The operation failed because of internal Kurdish defections and when it became clear that the United States would not follow through on its propaganda promises.[20]

Overall, the benefits of successful secret propaganda revolve around the "facts on the ground," that is, secret propaganda may generate greater local credibility than an official (or white) propaganda outlet. In addition, secret propaganda may be the only way for the United States to counter propaganda against it. This may be especially true when the adversary has had success in its propaganda against the United States. This was the case during the Cold War and may be the case now in the counterterrorism fight. It is certainly true that truthful information is essential to counter false information, but the truth may often need the assistance of secret propaganda to overcome preconception, misconception, and prejudice.

An additional benefit of secret propaganda is its possible effects on the actions of leaders. Successful secret propaganda may manipulate the attitudes and perceptions of elites in ways that are desired by the U.S. government. Allied propaganda during the Kosovo war, for example, was directly responsible for Serbian strongman Milosevic's decision in June 1999 to accept NATO's terms for settling the conflict, motivated by his belief that NATO was poised to launch an even more massive bombing campaign if its terms were rejected.

On the negative side, secret propaganda may result in unforeseen consequences that could be detrimental to U.S. interests. One unintended and dire effect of secret propaganda is blowback, the domestic consequences of intended propaganda (and other covert action) program abroad. The issue is particularly relevant today because information flows around the globe at an unprecedented rate with the growing use of computer technology and the Internet. A disinformation campaign abroad, for example, may be reported at home by the American press or American scholars as true, as was the case with the *Wall Street Journal* in 1986 in the Libya operation. This kind of domestic consequence almost certainly skews the domestic political debate and possibly affects its outcome. Activities that may result in blowback also contravene the terms of the 1991 Intelligence Authorization Act, which stipulates that the government will refrain from engaging in actions that may directly or indirectly influence American domestic politics, public opinion, or the media.[21]

Furthermore, there are ethical and moral arguments against secret propaganda programs, especially those that use the press as their conduits. One moral

argument holds that secret propaganda undermines the free press, in that journalists in free countries should not be bought and their media corrupted for questionable gains by the U.S. government. Another ethical argument says that recruiting foreign journalists may backfire on the United States. It is possible, for example, for foreign journalists, under covert circumstances, to turn on the United States and reveal their covert recruitment, thus providing pretexts for propaganda against the United States and embarrassment to the government.

THE BALANCE SHEET

Although propaganda—the dissemination of information for strategic objectives—is part of any government's repertoire, secret propaganda stands on its own to mean the use of information to manipulate, control, or direct a target's preferences in specific ways. The secrecy associated with it gives such propaganda its notoriety and sinister veneer. Though there are legitimate policy reasons for employing secret propaganda to implement aspects of American foreign policy, its success depends to a large extent on highly specific and narrowly construed factors.

On balance, secret propaganda works well when driven by a foreign policy consensus on its utility and when designed in ways commensurate with its intended objectives, as was the case in many of the secret propaganda efforts during the Cold War. Secret propaganda that does not elicit broad-based elite support or that is designed poorly, such as the recent efforts in Iraq and Afghanistan, will almost certainly backfire on the government and result in policy failure.

NOTES

1. See Jeff Gerth, "Military's Information War Is Vast and Often Secretive," *New York Times*, December 11, 2005.

2. Walter Jajko, "It's Propaganda Time," *Los Angeles Times*, December 2, 2005, p. 13.

3. Testimony of Karen Hughes, Under Secretary of State for Public Diplomacy, Before the House International Relations Committee, November 10, 2005.

4. Office of the Secretary of Defense, *Quadrennial Defense Review Report* (Washington, DC: U.S. Department of Defense, February 6, 2006), pp. 91–92.

5. Gerth, "Military's Information War Is Vast." Also see Jajko, "It's Propaganda Time."; Jeff Gerth and Scott Shane, "U.S. Said to Pay to Plant Articles in Iraq Papers," *New York Times*, November 30, 2005, pp. A1, A18; and "Propaganda Bombards Iraqis on Both Sides," *Associated Press*, September 17, 2005.

6. David S. Cloud and Jeff Gerth, "Islamic Leaders Were Paid to Aid U.S. Propaganda," *New York Times*, January 2, 2006, pp. A1 and A6.

7. Department of State Report on the Conference of Chiefs of Mission, February 21, 1951; U.S. Embassy in Tehran dispatch 1023 on using anti-Soviet materials within Iran,

May 29, 1953; and National Security Council, *Memorandum on U.S. Objectives and Policies with Respect to the Near East*, July 6, 1954.

8. Michael A. Turner, *Historical Dictionary of United States Intelligence* (Lanham, MD: Scarecrow Press, 2006), pp. 167–68.

9. Ibid.

10. Ibid., pp. 38–39.

11. Ibid., p. 168.

12. Gerth, "Military's Information War Is Vast"; Jajko, "It's Propaganda Time"; Gerth and Shane, "U.S. Said to Pay to Plant Articles"; and "Propaganda Bombards Iraqis on Both Sides."

13. See Deborah G. Berger, *Toward a Revolution in Intelligence Affairs* (Santa Monica, CA: RAND Corporation Technical Report, 2005), pp. 116–24.

14. Trevor Barnes, "Democratic Deception: American Covert Operations in Post-War Europe," in David A. Charters and Maurice A. J. Tugwell, eds., *Deception Operations: Studies in the East-West Context* (London: Brassey's, 1990), pp. 297–305.

15. Ibid.

16. David A. Charters, "Breaking Cover: The Bay of Pigs Intervention," in *Deception Operations: Studies in the East-West Context* eds. David A. Charters and Maurice A. J. Tugwell (London: Brassey's, 1990), pp. 353–55.

17. Jeff Gerth, "Military's Information War Is Vast."

18. "Farming out Psyops," *Intelligence Online*, June 17, 2005; Renae Merle, "Pentagon Funds Diplomacy Effort," *Washington Post*, June 11, 2005; and Dean Calbreath, "SAIC to Join Pentagon's Media Blitz," *San Diego Union Tribune*, June 18, 2005.

19. James Bamford, interview on National Public Radio, December 2, 2005.

20. Gerth, "Military's Information War Is Vast"; Jajko, "It's Propaganda Time"; Gerth and Shane, "U.S. Said to Pay to Plant Articles."

21. Intelligence Authorization Act, *Congressional Record* (28 June 1991), p. S9212.

6

POLITICAL ACTION AS A TOOL OF PRESIDENTIAL STATECRAFT

WILLIAM J. DAUGHERTY

THE INTELLIGENCE DISCIPLINE OF COVERT ACTION HAS been a policy staple of every post–World War II American president, Democrat or Republican, and most often employed against countries and organizations that were or are hostile toward the United States or U.S. interests. But covert action didn't start with the Cold War; indeed, a number of earlier presidents, going back to George Washington, also relied on what we would call covert action to achieve foreign policy objectives. Thus, covert action is traditional tool of presidential statecraft, the purpose of which is, simply stated, to influence a foreign audience either to do something, or to refrain from doing something, in a direction that coincides with American foreign policy objectives. Put differently, covert action is applied, by specific presidential direction, to compel the target audience to change its policies or its behavior. The target audience might be a foreign government, a foreign nation's general population or distinct part of a population, or members of a hostile nongovernmental organization, such as a narcotics cartel or terrorist group.

Individual covert action operations are managed very much like intelligence collection or counterintelligence operations in that foreign nationals recruited and directed clandestinely to perform a specific mission, usually the provision of confidential information. The difference is that, whereas all aspects of a collection or counterintelligence operation are to remain secret, a covert action operation must ultimately produce some result that is clearly apparent, or overt, at least to the target audience (if not the wider public) if it is have any influence or effect. Although the result must be visible, the sponsorship, for example, the government or intelligence service, of the persons or group that generated the apparent result must remain hidden so as not to undermine the result's credibility with the target audience. In sum, the identity of the sponsor is actually the secret, not the

operation itself. For example, if a respected labor leader in a country whose population was generally unsympathetic to the United States were to organize a general strike to emphasize the incompetence of his government, neither he nor the strike would be credible if it were known that the U.S. government was secretly paying him to perform this act.

Purely clandestine operations that are run either to collect sensitive information or to serve a counterintelligence objective are legally considered as routine missions of the U.S. intelligence community. As such, the individual intelligence agencies within the community possess continuing legal authorities to conduct these operations, a great deal of institutional latitude in how they do it, and a fairly low level of congressional oversight. Conversely, covert action programs are not routine intelligence activities: they must have special authorizations to meet federal law requirements, they are denied a good deal of the policy and operational flexibility that other intelligence operations enjoy, and they receive intense oversight from not only Congress but also the National Security Council. Arguably, because they are implemented explicitly to support a president's foreign policy initiative, covert action programs are not even "intelligence" in nature, even though they are executed by the Central Intelligence Agency (CIA) and rely on clandestine methodologies. These differences ultimately remove covert action programs from the realm of general intelligence activities and transform them into highly sensitive instruments of presidential policy.

In essence, covert action programs are secret adjuncts to a particular foreign policy established by the president and employed to support overt policy implementation measures (e.g., diplomacy, trade favoritism or sanctions, foreign aid, military force, training initiatives, and loan guarantees or grants). It is the president, advised by the National Security Council, who decides whether a policy will have a covert component and, if so, how that component will be used. For each covert action program, under which dozens or even hundreds of individual operations may be run, federal law dictates that the president sign a document declaring that he "finds" that the covert action program is necessary for national security purposes. This finding (as it is known in the parlance) spells out the objectives and implementation limits of each program, sets a program budget, defines the role of the CIA and any supporting agencies in executing the program, and includes a risk versus gain assessment. Furthermore, all findings must be sent to the intelligence oversight committees in Congress within forty-eight hours of the president signing the document. Once begun, covert action programs receive nearly continuous scrutiny from CIA senior management, Congress, and the president and his national security team. This oversight is conducted until the program is abolished, a move that again requires a presidential signature. These extra measures necessary to initiate, execute, and terminate covert action programs truly make them "presidential" in all respects.

Covert action programs fall under one of four general operational categories: propaganda, political action, information warfare, and paramilitary operations. Political action programs, the focus of this chapter, generally seek to achieve

influence through covert activities that involve the manipulation, legitimate or otherwise, of a foreign nation's political and/or economic system, with the instigating hand of the U.S. government remaining hidden from view. Political action operations are always provocative to some degree, ranging from operations that slightly irritate (e.g., paying a few individuals to carry protest signs in front of a government office or bribing public officials) to the highly antagonistic and hostile (e.g., flooding a country with counterfeit currency or creating a major strike to cripple the economy and undermine the ruling regime). Regardless, political action operations, whether directed at a nation's political institutions or its economy (and often both), seek to change the behavior or policies of a government. Such meddling is contrary to international law and the United Nations Charter and may, if compromised with the sponsorship of the American government exposed, generate many problems, both political and practical, for the president at home and abroad.

But offsetting this risk—and hence its attractiveness to presidents—is the fact that operations that covertly manipulate a country's political processes or economic system are usually much less costly than other forms of pressure, especially military force. For example, if a covert political action program to oust Panamanian dictator Manuel Noriega in 1989 had been attempted and succeeded, the financial and political costs of such would have been far less than the costs (including humanitarian) of using the U.S. military to invade and occupy the country until Noriega was captured.

American history is replete with examples of presidents authorizing secret activities intended to foster and further American interests at the expense of foreign governments. In point of fact, George Washington used covert action programs in addition to intelligence collection operations during the American Revolution and continued doing so after his election to the presidency in 1791 to secure the fledgling democracy. Arguably, the first use of covert action in the new administration was not against an overseas government but against the sovereign governments of Native American tribes.

Once in office, Washington was abetted by his secretary of state, Thomas Jefferson, in implementing a covert action program—a classic example of a political action operation—intended to create confidence and goodwill with various tribes whose lands lay between the settled East Coast and the interior of the continent, awaiting further exploration. Jefferson's objective was to lay the foundation for the U.S. government eventually to acquire their lands for the development or construction of inland transportation systems, such as roads, bridges, and canals, an infrastructure vital to the movement of commercial goods and people within the country. The need to grow the economy was critical to sustaining the faith of the Americans in the newly created democracy, the permanence of which was by no means assured just because the U.S. Constitution was ratified. Quite simply, if Americans were not better off economically under the new Constitution, there would little reason for them to continue to support it. Gaining access to tribal lands for the movement of goods, as well as to encourage

the migration to and settlement of the West was, hence, an important part of Washington's economic policy.

The methods Washington and Jefferson employed are easily recognized as basic political action tactics. First, the secretary of War was given visible responsibility for this program, putatively acting autonomously to insulate the president and secretary of State from any negative consequences that might occur. The War secretary then proceeded, through the help of clandestine agents, to bribe tribal chiefs, selectively dole out financing for trading posts and other businesses, extend (or threaten to foreclose) loans granted to tribal leaders, and manipulate the chiefs' human foibles (here, greed) to run them into heavy debt. Owing monies that they had no way of repaying left the tribal leaders vulnerable to exploitation by government agents, who agreed secretly to swap tribal debts for treaties transferring Indian land titles to the United States.

When Jefferson acceded to the White House, he was bedeviled by the predatory actions of the Barbary pirates, seagoing thugs who plundered American commerce in the western Mediterranean and captured American sailors for ransom. Jefferson's solution was the same that later presidents, including Dwight D. Eisenhower, John F. Kennedy, and Richard M. Nixon, found so attractive—implementing a political action program to undermine covertly the offending government (the Tripolitan Pasha) and affect a change of regime by placing a rival on the throne. Jefferson's scheme also involved bribery, secret funding of opposition groups, and a small paramilitary operation conducted by U.S. Marines. The Pasha, seeing the writing on the wall, decided to deal with Jefferson, resulting in an accord that halted acts of piracy against the U.S. merchant fleet and released the American hostages, while allowing the Pasha to retain his throne.

Covert actions, particularly political/economic action programs, were employed through the mid-1800s as America expanded westward, to gain land for the United States from European colonial powers and neighboring Mexico. Under James Madison's direction, two territorial administrators infiltrated secret agents into the Florida panhandle, at the time under Spanish control, to foment a rebellion that would appear to be the actions of local, pro-U.S. residents. The anticipated Spanish reaction would then provide the pretext for the president to order the occupation of the land by U.S. troops to protect lives and property, followed by a proclamation granting the locals their proclaimed wish for independence from Spain. The operation relied on individuals who, in today's intelligence lexicon, would be labeled "agents provocateur" and who were well supplied with secret funds and used a clandestine communications system to coordinate their schemes. A supposedly spontaneous insurgency against the Spanish did break out, with the rebels declaring independence and asking for assistance from the American government. Madison responded by proclaiming that west Florida was actually already a U.S. possession by dint of its (rather suspect) inclusion with the Louisiana Purchase, and soon the Stars and Stripes flew over Pensacola and Mobile.

Madison followed this land expansion with similar covert tactics (i.e., a spontaneous uprising and call for independence) from pro-U.S. inhabitants in eastern Florida, to acquire that territory before the British could seize it from the steadily weakening Spanish empire. His successors—James Monroe, John Quincy Adams, and Andrew Jackson—all employed elements of covert political action operations in their policies toward Mexico. Monroe maneuvered to reduce British influence with the Mexican regime, and Jackson attempted to induce the Mexicans to sell or cede land north of the Rio Grande to the United States. Bribery, support for underground opposition groups, inflammatory propaganda, the public dissemination of erroneous information (disinformation, in espionage parlance), and secret slush funds were all covert methods set in motion by these presidents. That Jackson was ultimately unsuccessful in gaining any Mexican land does not obviate the fact that he carefully and skillfully employed political action operations to further his overt foreign policy.

In an interesting parallel to a large covert political action program initiated in the 1980s under President Ronald Reagan that used a variety of means to deny sensitive emerging technologies to the Soviet Union, Abraham Lincoln established a clandestine network in Europe to prevent those nations from providing much-needed military supplies to the Confederate States during the Civil War. The complex program began with the collection of raw intelligence, the analysis of which identified individuals and companies secretly trading with the South. Political action operations were then run against the traders to disrupt the production of the war matériel, sabotage the factories, and intercept the matériel en route to the Confederate States. Knowing that the Union navy could not always snare the South's blockade runners, waging a covert interdiction campaign in Europe to prevent war matériel from being loaded on a Confederacy-bound ship in the first place proved an effective and economical way to deny the South vital war-making capabilities.

Prior to the Civil War, American presidents essentially used covert action in general and political action operations in particular to expand the land territory of the nation and protect American lives and commerce from foreign interference. But within two decades of the ending of the American insurrection, and well before the United States became a world military force, presidents began using these covert methodologies to strengthen foreign commercial ties, protect American economic interests, and expand international trade. In the 1880s, the American government became cognizant of the tremendous economic potential of Asia as a source of raw materials and a destination for the export of finished goods. It became the goal of presidents to open these markets to trade and to protect the markets once established. A concomitant objective was to reach agreements with Asian regimes for coaling stations for the U.S. Navy's growing Asiatic fleet. Korea drew the interest of the navy and, hence, of President Chester A. Arthur (not a president one usually associates with an aggressive foreign policy), early in that decade for both a trading partner and a refueling post. But Japan and China

had squared off over which was to exercise the dominant political and economic influence over the Korean Peninsula, leaving Korea much like a fish caught between two cats. Arthur relied on covert political activities, particularly the supply of arms and funds to a Korean group interested in upsetting the pro-Chinese regime that held power (with the U.S. involvement remaining under the table), to drive a wedge between Tokyo and Beijing in hopes of creating and then filling a power void. A quick-rising squabble between France and China distracted the latter and provided a fortuitous opening for the American-supported clique, which then moved into power.

Under President Benjamin Harrison, America's annexation of Hawaii, whose natural port at Pearl Harbor was a matter of strategic import for the Asiatic fleet, was the consequence of a political action operation bearing similarities to Madison's grab of west Florida. It likewise involved, in 1893, the clandestine fomenting of a "popular" insurrection that portended bloodshed and justified intervention to protect American diplomatic facilities and citizens. Navy sailors and marines occupied Hawaiian government buildings, and the American ambassador soon thereafter declared the establishment of a provisional—and pro-American—government.

But it was, of course, the Cold War and the creation of the CIA that truly made covert political action a critical component of presidential statecraft. Throughout the Cold War, it was the fundamental objective of the United States to (1) counter Soviet expansionary policies; (2) support pro-West governments that were targets of Soviet subversion; and (3) weaken or undermine foreign governments that had fallen into the Soviet orbit. (Policies of transforming oppressive regimes into democracies had to wait until the presidencies of George H. W. Bush and his son, George W. Bush.) The attraction for American presidents in employing political and economic covert actions against the Russian bear was that it permitted the U.S. government to apply a varying degree of pressure against the Moscow regime, but to do so without generating a clear and direct threat to core Soviet interests that might eventually invite a military response. Because covert action programs used a broad spectrum of capabilities that allowed presidents to calibrate the intensity of the pressure felt or perceived by the Soviet leadership, the interests of the United States were protected and advanced but without backing the Soviets into a corner that might have left them no recourse but war. (Of course, the Soviets were concurrently doing the same things against the United States, using the term "active measures" in place of covert action.)

Although at first rather reluctant to open an intelligence war against the Soviet Union, which had been, after all, America's ally in the recent world war, by 1947 President Harry S. Truman had become convinced that Soviet hostility toward the United States, the Western democracies, and capitalist systems would only increase, ultimately threatening democracies and nations seeking to become democratic. To counter Soviet subversive operations in regions considered vital to U.S. national security, Truman implemented overt policies such as the Truman Doctrine (for Greece and Turkey) in March 1947, and the Marshall

Plan (for the reconstruction of Western Europe) just three months later. But overt programs intended to strengthen democratic political systems and rebuild devastated economies in Europe and the Near East were also judged to be insufficient when considering the scope and depth of Soviet covert machinations to undermine those same countries. Under Truman's personal initiative, his newly established National Security Council (NSC) drew up its first national security directive—an order for the CIA (created concurrently with the NSC by federal statute) to counter Soviet political and economic subversive programs in Italy and France, operations by which the Stalinist regime in Moscow sought to acquire control of those governments through manipulation of legitimate electoral processes.

To be sure, there were precedents from which one could learn. Elections in Eastern European countries following the war found the local communist parties legitimately winning seats in those parliaments, from which party members were then chosen to fill key Cabinet positions in the government. With covert assistance from Moscow, the democratic processes were subverted from within (Czechoslovakia was particularly instructive), resulting in the establishment of oppressive pro-Soviet communist regimes. In France and Italy, Soviet agents were likewise seeking to gain control of those elements of society that are fundamental to democracy—political parties, newspapers, labor unions, publishing houses, student groups, and more—through the provision of nearly unlimited funds and then employ these societal influences as front organizations for Soviet intelligence to use to corrupt the democratic processes.

NSC documents from 1947 and 1948 show that the Truman administration viewed a victory for the French and Italian communist parties as an unacceptable outcome and, should that happen, reached the conclusion that all governments in Western Europe would be menaced. The CIA was given the responsibility of countering the Soviet operations, in part by political action—the provision of secret funding to individual candidates for political office as well as to the multiple political parties. In this, neither the U.S. government nor the CIA had a preferred candidate or party. The funds, millions of dollars, were given liberally to groups, organizations, unions, and politicians across the political spectrum, from the far right to the left of center. It mattered not so much who won, but who had to be defeated. Ultimately, between overt U.S. policies and the covert program, the communists lost at the polls. Still, it terms of the role that political action operations played in the greater scheme of things, it is important to understand that the millions of dollars in covert funding constituted only a small percentage of the monies expended in the overt diplomatic programs meant to strengthen governmental institutions and to rebuild the economies devastated from war. Covert action programs, certainly including political and economic operations, are most effective when supporting well-established overt policies, and the operations in Italy and France are proof of this. The perceived need to secretly fund Italian politicians and parties continued through the administration of Lyndon B. Johnson, ending only in 1967.

Perhaps the most familiar—or notorious—political action operations are those in which the president directs the CIA to oust a foreign government or regime. Again, the idea is to make it appear as though local opposition groups act on their own initiative and through their own resources. Presidents Eisenhower, Kennedy, and Nixon each issued orders to the CIA to do overthrow regimes deemed to be politically too close to the Soviet Union, but with varying degrees of success. Operations to reverse regimes in Iran and Guatemala managed to achieve their objective, but similar efforts in Indonesia, Cuba (after paramilitary operations failed in each), and Chile did not. Kennedy furthered toyed with the idea of ordering political action programs to unseat regimes in Santo Domingo and British Guyana as did Reagan early in his administration with Surinam.

The covert overthrow of a foreign regime by the United States is never as easy as its proponents seem to believe, nor are successes truly positive or unalloyed in the long term. For many intelligence professionals, the overthrow of the Iranian regime of Mohammed Mossadeq in 1953 was a double-edged sword, for the ease with which it seemingly occurred served to mislead future presidents and CIA directors into attempting similar operations with less fortunate results. In the case of Iran, the fact is that the CIA itself did not cause the overthrow of Mossadeq. What the CIA did was to provide, in essence, a push at the margins of an already developed and much larger indigenous political movement unhappy with Mossadeq and his policies. It is unknown whether the anti-Mossadeq forces would have prevailed had the CIA not stepped in at a key moment, but it is beyond doubt that the CIA as an institution did not itself effect the change. Indeed, the operation at first appeared to be an abject failure, and it was only the fortuitous appearance of a popular Iranian general to rally the mobs at a critical moment that brought about the ouster of Mossadeq. It is not an oversimplification to say that the Americans contributed just the right amount of pressure, at just the right moment, with just the right people. Said differently, the operation succeeded mostly (or even only) because of luck.

Yet the lesson the CIA and the Eisenhower (and later Kennedy) administration took away from the Iranian program was that the reversal of hostile regimes was nothing particularly difficult; that American ingenuity and righteousness of purpose were enough to prevail. Interestingly, the one person who realized differently was the man who orchestrated the Iranian program, Kermit Roosevelt. Asked to lead the next such operation, the removal of Guatemalan leader Jacobo Arbenz, barely a year later, Roosevelt declined and left the agency. That the Guatemalan operation, a blend of paramilitary, political action, and propaganda operations went well further solidified the belief in the Washington circle that the United States could replace governments at will and without fear of failure.

After the Guatemalan program, the Eisenhower administration took aim at the Indonesian government of Sukarno, who announced his intentions of allowing Communist Party members to hold positions in his Cabinet. Eisenhower, duly alarmed at the prospect of a pro-Soviet regime in that county, authorized a robust

covert action program, including operations aimed at manipulating the political and economic processes, to remove Sukarno from power. This effort failed miserably, with the consequence that Sukarno's hold on power was stronger. An astute, objective student analyzing this program might have reached the conclusion that maybe, just maybe, political action operations to change an entrenched regime might not be as easy nor as useful as thought. But with the apparent successes of Iran and Guatemala in the background, the lessons of Indonesia were lost.

It is instructive to note that the definition of *success* as applied to a political action program, especially one in which the change of a regime through subversive measures is the objective, can be elusive. Eisenhower, Kennedy, and Nixon each believed that success constituted the replacement of a pro-Soviet or potentially pro-Soviet government with a right-wing, pro-American regime. And in the short term, that was perhaps so. But over the longer run, arguably more harm was done. The hapless Mossadeq was replaced by a monarchy that grew more oppressive and dictatorial over the years, itself eventually overthrown by indigenous elements, transforming America's most important ally in the Middle East into radical Islamic fundamentalist state that has now waged a war of terrorism against America for a quarter century. Although communist forces were thwarted in Guatemala in 1954, the resulting oppressive right-wing military dictatorship murdered hundreds of thousand of its own citizens over the next forty years, leaving an impoverished nation in its stead.

Chile was the target of covert electoral manipulations beginning with Kennedy, who sought to forestall socialist or communist regimes by directing the provision of secret funds to several Chilean political parties and, especially to one presidential candidate, Eduardo Frei. The program continued through President Nixon, who at one time toyed with instigating a military coup to prevent the election of socialist Salvador Allende. When this proved unfeasible and Allende was elected, Nixon turned his efforts toward destabilizing the new regime. Included in his bag of tricks were monies given to political parties and candidates, payments to various mass media outlets to produce political advertisements or messages, and funds to social and professional organizations—labor unions, student groups, women's clubs, and business and civic associations. In the end, the military acted unilaterally, instigating a coup that left Allende dead and the government in the hands of an oppressive right-wing military cabal that endured for two decades.

But not all political action programs are failures. The CIA managed a number of covert political action operations against the Soviet Union, some for nearly the length of the Cold War. These programs picked up strength and importance during the administration of Jimmy Carter, including operations that fostered the printing and underground distribution within the Soviet Union of prohibited political tracts, the writings of banned Russian authors like Aleksandr Solzhenitsyn and Boris Pasternak, and religious works (Bibles and Korans). Along with the infiltration of printed materials, these political action operations provided, through secret channels, desktop publishing equipment to Soviet

dissidents to print and disseminate their writings, known as *samizdat*, within the Soviet Union. Additionally, operations funded Soviet exiles in Western Europe, enabling them to write and publish books, journals, and monographs that, though intended primarily for distribution within émigré circles, likewise found their way clandestinely with to readers inside the Soviet Union. An adjunct initiative known as the Nationalities Program, funded the printing and distribution of journals and pamphlets directed towards the non-Russian ethnic minorities in the Soviet Union, keeping alive their history, culture, and language at a time when the Soviet government was attempting to suppress them. Other CIA political action programs in Europe funded human rights and prodemocracy organizations as part of a larger effort to counter anti-Western Soviet propaganda. These programs and more were continued and expanded during the administration of Ronald Reagan, effectively and inexpensively applying pressures on the Soviet government that contributed to the ultimate demise of the Soviet Union.

But perhaps the most successful political action program ever was a broad-based effort to undermine the legitimacy of the Polish military government that came to power in 1980 while concurrently supporting the independence movement headed by Polish labor union Solidarity. If a critical attribute of any covert action program is that it would, if exposed, meet with the approval of the American public, this was one such program. Although much of the program remains classified, despite its overwhelming success, elements of it have come into the public eye.[1]

As the end of the Carter administration drew near, it was faced with the Soviet Union pressuring the Polish government to outlaw Solidarity and its supporters, as well as threatening to move its military across the border if the Polish power structure failed to contain the growing influence of the union. In response, Carter directed his National Security Advisor, Zbigniew Brzezinski, to advise the Vatican that the United States had clandestine intelligence resources available to aid Solidarity. Moreover, with European governments reluctant to openly confront the Soviet Union over its aggression, Brzezinski bluntly asked Pope John Paul II if he would consent to joining with the United States to isolate economically, culturally, and politically the Soviets if they openly intervened in Poland. The Pope would and did.

The Reagan administration thus inherited an expanding covert political action program that first deterred a Soviet military intervention in Poland (similar to the Soviet invasions of Hungary in 1956 and Czechoslovakia in 1968) and then enabled Solidarity and other underground organizations to survive and resist the martial law government of Gen. Wojciech Jaruzelski. But the CIA's covert operations did not end with just Poland: Reagan believed that if Poland was able to throw off the communist system and emerge as a free and democratic nation, the other five Eastern European countries would follow. The Polish program thus expanded into a worldwide confrontation of the legitimacy of the communist governments of Eastern Europe and the Soviet Union itself. Poland held its first free elections in 1989, and within two years not only were Eastern European countries free of Soviet domination, but the Soviet Union as a political system

disappeared into the dustbin of history. Of course, Eastern Europe did not gain its independence nor did the Soviet Union collapse solely because of the covert action operations initiated by the Reagan administration, but these missions did fulfill their intended goal and then some, supporting a vast array of overt United States political, economic, and military policies that collectively made it impossible for Moscow to continue the Cold War.

This abbreviated introduction to covert political action programs operations is meant neither to convince the skeptical of their efficacy nor to provide support to those who see them as a solution to difficult or seemingly insoluble foreign policy issues.[2] Truman and Eisenhower employed political action operations against the Soviet threat with mixed results. Truman's use of covert action in Italy and France must be judged as highly successful, whereas the long-term consequences of the Iran and Guatemalan operations, as well as the clear failure of the Indonesian venture, place into question the wisdom of Eisenhower's decisions to use covert methods against those regimes. Kennedy's efforts in influencing the Chilean elections was successful only in the short term, with a socialist government eventually coming to power despite his efforts, as well as Johnson's, and Nixon's use of multiple political action operations to forestall it. Similarly, Kennedy's intense efforts to overthrow the Cuban regime of Fidel Castro were not only unmitigated failures but might well have placed his administration in serious jeopardy, had the operations become public knowledge during his tenure in office. Unrecognized by many historians, Carter's reliance on covert programs, political action especially, was more successful than not, especially in that he laid the foundation for many of Reagan's programs against the Soviet Union directly and in countering Soviet interventions in places like Afghanistan and Central America.

Whether or not political action programs are an appropriate tool for the president in implementing foreign policies depends on a number of factors, not the least of which is the ability of the president and the national security team to recognize and accept the limits of any covert action program. Certainly it should be clear that these political action operations are not suitable for crisis resolution; rather, they are most wisely employed in consonance with a thoughtfully developed, comprehensive, foreign policy with well-defined objectives implemented in a methodical manner. Successful foreign policies are never the responsibility of just one agency of government, and certainly not intelligence agencies. But covert actions that influence the political or economic systems of target audiences may, when wisely employed, serve a president and the country well.

NOTES

The author thanks Matthew Easterwood, presently a student at Stetson Law School, for his research assistance with this chapter.

1. Robert M. Gates, a former director of the CIA, has provided some detail in his memoir, *From the Shadows: The Ultimate Insider's Story of Five Presidents and How*

They Won the Cold War (New York: Simon & Schuster,1996), which was cleared for publication by the CIA. Other partial accounts have appeared in Zbigniew Brzezinski, *Power and Principle: Memoirs of a National Security Advisor 1977–1981* (New York: Farrar, Straus & Giroux, 1985); and Carl Bernstein and Marco Politi, *His Holiness, John Paul II and the Hidden History of Our Time* (New York: Doubleday, 1996), on which the CIA will not comment. This is unfortunate in that the story is generally now in the public domain, but also at a time when the CIA and the intelligence community are under serious attack, a story that is clearly a great success would only redound to the benefit of the CIA.

2. Mention of more recent covert programs, including political and economic action operations, which might provide more enlightenment for this chapter, is precluded by continuing classification of programs after the Reagan era and the CIA's requirement that this author clear his writings with them prior to publication.

7

COVERT ACTION AND THE PENTAGON

JENNIFER D. KIBBE

THE TERRORIST ATTACKS ON SEPTEMBER 11, 2001, brought about a number of changes in the U.S. national security outlook, not the least of which was a renewed willingness to consider covert action as a policy option. During this same period, the single most significant change in the military services has been the expansion (in both size and responsibility) of its special operations forces. The concurrence of these two trends has led to a blurring of the distinction of whether military units are conducting covert operations and has raised questions about congressional oversight. The *Quadrennial Defense Review* issued by the Pentagon in February 2006 stated unequivocally that special operations forces would be leading the war on terror, making it that much more important to understand the issues raised by potential military involvement in covert action.

Covert action is defined in U.S. law as activity that is meant "to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[1] Covert actions are thus legally distinct from clandestine missions: "clandestine" refers to the tactical secrecy of the operation itself, and "covert" refers to the secrecy of its sponsor. Although most often associated with the assassination of leaders or the overthrow of a government, the category of covert action can include a wide range of activity, from propaganda and disinformation to political influence operations, training and support for foreign military forces, to paramilitary operations. Historically, the Central Intelligence Agency (CIA) has been the main agent of U.S. covert action, but the growth of special operations forces over the past two decades and their ability to conduct direct action operations has raised new questions in the debate over congressional versus executive control of covert action.

EVOLUTION OF SOCOM

The military's unconventional warfare operations, whether covert or clandestine, are part of the U.S. Special Operations Command (SOCOM), a relatively new command that has now been designated as the leader in the U.S. war against terrorism. Although their roots can be traced to various World War II forces, including the Office of Strategic Services (OSS), air commandos, Scouts, and Raiders, American special operations forces were first really built up in Vietnam as a result of President Kennedy's interest in using the Green Berets to conduct unconventional warfare. However, these forces were somewhat resented by the regular troops and officers who felt that the armed forces' conventional training and approach to warfare had always been good enough before and that there was no need to introduce any sort of "special" forces. Thus, when the end of the war in Vietnam led to severe budget cuts, every one of the armed services drastically cut its special operations units.

The event that caused the pendulum to swing back the other way was the failed mission to rescue the American hostages in Iran in 1980. Because the United States had no standing counterterrorist task force, the necessary personnel and equipment were drawn from the various services, leaving a significant gap in overall coordination. When two aircraft collided in the desert outside Tehran, eight members of the operation died and the rest were forced to turn back without attempting to rescue the hostages, leaving behind three intact helicopters to boot. Within weeks, a commission had been formed to review the failed operation and determine how to improve the United States' ability to run such operations in the future. The Holloway Commission, named for its chair, Chief of Naval Operations Adm. James Holloway, emphasized the uncoordinated nature of U.S. special operations, as well as the lack of any independent review of the operational plans and the poor intelligence support. The commission's recommendation for the creation of a Counterterrorist Joint Task Force was adopted and implemented over the next several years.

The early 1980s saw increased funding for special operations forces, an expansion in personnel and the creation of the Joint Special Operations Command (JSOC, pronounced "jay sock"), whose goal was to provide increased coordination. The first real operational test of the improvements was Operation Urgent Fury, the 1983 invasion of Grenada. Special operations forces, including Navy SEALs, Army Rangers, and members of Delta Force, were directly involved in seven of the operation's eight targets, of which only two were fully successful. Three of the operations were costly failures, with special operations forces incurring heavy casualties as a result of poor planning, coordination, and intelligence.

The failures at Grenada fueled a new round of calls for reform, and not just of special operations forces. This time, however, those interested in reform included some on Capitol Hill. This round of investigations eventually resulted in the Department of Defense Reorganization Act of 1986, also known as the

Goldwater-Nichols Act, which substantially strengthened the power of the chairman of the Joint Chiefs of Staff and the unified combatant commanders (the commanders of the various regional theaters). The element of the Goldwater-Nichols Act that most affected special operations, though, was the subsequent Nunn-Cohen amendment that, most importantly, established SOCOM. Although SOCOM was established as a supporting command, meaning that it could not plan or execute its own independent operations and could only operate in support of other commands' operations, the new legislation still represented a significant step forward in the coordination and enhancement of special operations forces. The Nunn-Cohen amendment also specifically laid out in law, for the first time, the types of operations that would be included under the rubric of special operations: "Direct action, strategic reconnaissance, unconventional warfare, foreign internal defense, civil affairs, psychological operations, counterterrorism, humanitarian assistance, theater search and rescue, [and] such other activities as may be specified by the Secretary of Defense."

In the four major conflicts involving the United States since Grenada (the invasion of Panama, the Gulf War, the Afghanistan war, and the Iraq war), special operations forces have proven to be increasingly effective and useful.

SPECIAL OPERATIONS FORCES TODAY

SOCOM is comprised of both units that conduct overt or "white" operations, and those that conduct "black" operations, including both covert and clandestine missions. Those involved in white special operations include Army Special Forces (Green Berets), most Ranger units, most of the Navy SEALs, and numerous aviation, civil affairs, and psychological operations units. These white special operators are largely involved in training selected foreign forces in counterterror, counterinsurgency, and counternarcotics tactics; helping with various civil government projects; and disseminating information to foreign audiences through the mass media. The black operators fall under JSOC, which commands the elite units of each service's special operations forces, including Special Forces Operational Detachment—Delta (Delta Force), Naval Special Warfare Development Group (DEVGRU, or SEAL Team 6), the Air Force's 24th Special Tactics Squadron, the Army's 160th Special Operations Aviation Regiment and 75th Ranger Regiment, and a highly classified Intelligence Support Activity team (known as ISA, or more recently as Gray Fox, although its name changes frequently). These units (also known as special mission units) specialize in direct action operations such as hunting terrorists and rescuing hostages. Although it is generally understood that these units exist, the Pentagon does not officially acknowledge them.

From the beginning of his term, one of Secretary of Defense Donald Rumsfeld's chief priorities has been to transform the military from a large conventional force built to face another superpower into a leaner, more flexible, and

agile force capable of fighting the less conventional conflicts that have dominated the post–Cold War period. Though his desire to expand special operations was part of that original overall goal, it received a huge boost when at the beginning of the war in Afghanistan, the military's special operations units had to rely on CIA operatives to establish links to the Northern Alliance fighters. By all accounts, Rumsfeld was incensed and was determined to build up his special operations capabilities to eliminate any future dependence on the CIA.

That determination has gradually led to significant increases in funding, personnel, and authority for special operations forces. The FY 2007 defense budget called for special operations funding to grow to $5.1 billion, approximately $1 billion more than the previous year and double the amount allocated to them in 2001. The 2006 *Quadrennial Defense Review*, the Pentagon's main planning document for the next four years, aimed to increase special operations troops, which numbered about 50,000 at the beginning of 2006, by 14,000 through 2011, at a cost of nearly $28 billion. (Note that of the 50,000 current special operations forces, only approximately 10,000–13,000 are "trigger-pullers," i.e., those in the field involved in operations. The remainder are support and administrative staff.)

Beyond the actual numbers, Rumsfeld has also effected several substantive changes in the way SOCOM is run. First, he replaced those leaders of SOCOM who were, in his estimation, too cautious about the command assuming a more aggressive role in the war on terror. He also significantly increased SOCOM's authority by changing it from a supporting to a supported command, meaning that it could now plan and execute its own missions (if authorized by the secretary and, if necessary, the president). This change gave SOCOM a considerable amount of increased flexibility, because it meant the chain of command now went directly from SOCOM to the secretary, without having to go through a regional unified command (Southern Command, for example). This change could also be seen as giving the secretary increased control over special operations. Cutting out the regional commands, however, also presents an increased risk that special operations units may plan missions without taking sufficient account of possible regional repercussions.

In March 2004, after an intensive bureaucratic struggle, Rumsfeld was successful in his campaign to install SOCOM as the leader of the war on terror, ahead of the conventional forces whose leaders he perceived as too tentative. President Bush signed the new Unified Command Plan 2004, which designated SOCOM as the "lead combatant commander for planning, synchronizing, and as directed, executing global operations" in the war on terror (although it did leave the regional commanders in charge of counterterrorism operations in their own theaters).

An amendment to the defense authorization bill in October 2004 represented a further step along SOCOM's road to independence as Congress granted its forces the authority, for the first time, to spend money to pay informants, recruit foreign paramilitary fighters, and purchase equipment or other items from foreigners. Previously, only the CIA had been authorized to disburse such funds, meaning that special operations forces had to rely on the CIA to provide the funds for

various operations. One other significant step in the special operations forces' rise to prominence came in January 2006 when JSOC's headquarters was raised from a two-star to a three-star command, thus giving its chief more authority and influence in dealing with other military officers.

There is little doubt that Rumsfeld's vision for SOCOM is a long-term one. Indeed, in presenting the 2006 *Quadrennial Defense Review* to the press in February 2006, Rumsfeld described its emphasis on developing special operations forces as a necessary component of U.S. preparation for what he called the "long war" ahead against extremism. The review calls not only for significant increases in forces but also for increased training of conventional troops in "irregular" operations, such as counterinsurgency and stabilization operations, thus freeing up special forces operators for "more demanding and specialized tasks, especially long-duration, indirect and clandestine operations in politically sensitive environments and denied areas." In addition, the document states that for direct action, special operations forces "will possess an expanded organic ability to locate, tag and track dangerous individuals and other high-value targets globally."[2]

Also in February 2006, Gen. Peter Pace, Chairman of the Joint Chiefs of Staff, reportedly signed a new, classified counterterrorism strategy that orders the Defense Department to undertake a broad campaign to find and attack or neutralize terrorist leaders, their havens, financial networks, methods of communication, and ability to travel. According to the *New York Times*, the strategy document specifies that the effort to defeat terrorism requires "continuous military operations to develop the situation and generate the intelligence that allows us to attack global terrorist organizations."[3]

Another major facet of SOCOM's burgeoning role is its wide geographic scope. In the five years since 9/11, special forces operations have been reported in the Philippines, Malaysia, Georgia, Colombia, Indonesia, Pakistan, Yemen, Algeria, Morocco, Mauritania, Niger, Mali, Chad, Nigeria, and Jordan. Although most of the reported operations are of the white variety, usually involving counterinsurgency and counterterrorism training of indigenous forces, there is little doubt that with the Pentagon's stated goal of hunting down terrorists, black special operators are or will be active in many of those same countries.

SOCOM's growth in size, scope, and influence raises the questions of whether it is conducting any covert operations and of the degree and adequacy of congressional oversight of its activities.

LEGAL REQUIREMENTS

Congress first tried to assert control over covert action in the mid-1970s in reaction to revelations of U.S. involvement in the coup against Salvador Allende in Chile and assassination attempts against Fidel Castro. The Church Committee, named for Sen. Frank Church (D-ID), chair of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, conducted

an investigation that led to the establishment of permanent intelligence committees in both the House and the Senate. The Iran-*contra* scandal in the Reagan administration, however, highlighted important gaps in the new congressional oversight requirements. In response, Congress adopted more stringent provisions in the 1991 Intelligence Authorization Act, which is still the governing legislation on congressional oversight requirements. The act codified two requirements for any covert action. First, there must be a written presidential finding stating that the action is important to U.S. national security, which cannot be issued retroactively. Second, the administration must notify the intelligence committees of the action as soon as possible after the finding has been issued and before the initiation of the operation, unless "extraordinary circumstances" exist, in which case the president must fully inform the committees "in a timely fashion."[4]

The other significant feature of the 1991 Intelligence Authorization Act is that in response to the Reagan administration's use of the National Security Council to conduct covert action in connection with Iran-*contra*, it expressly applied the requirements to "any department, agency, or entity of the United States Government." In other words, Congress no longer assumed that only the CIA could or would conduct covert operations. The law also included, however, a few designated exceptions to the definition of covert action. Under the most significant one, "traditional . . . military activities or routine support to such activities" are deemed not to be covert action and thus do not require a presidential finding or congressional notification. Although the act itself does not define "traditional military activities," the conference committee report presenting the legislative history states that the phrase is meant to include actions preceding and related to hostilities that are anticipated to involve (conventional) U.S. military forces or where such hostilities are ongoing, whether U.S. involvement in the action is made public or not, as well as any military action where the U.S. role is apparent or to be acknowledged publicly.[5]

The interpretation of the "traditional military activities" exception has caused considerable controversy as the Bush administration relies increasingly on special operations forces in the war on terror. Covert operations conducted by special operations forces during wartime clearly do not require a presidential finding and congressional notification. The definition leaves a gray area, however, around the interpretation of the word *anticipated*. It is most commonly thought of in the literal sense of "preparing the battle space" and, in fact, the conference committee report of the 1991 law defines "anticipated" hostilities as those for which operational planning has been approved. Defense Department officials, however, have explained that under the Pentagon's interpretation, the language could refer to events taking place "years in advance" of any involvement of U.S. military forces. Critics contend that the Bush administration has been eager to shift more covert activity from the CIA to the military precisely because they see it as giving them more of a free rein.

But the Pentagon's interpretation of *anticipated* raises an obvious and important question: In prosecuting the war on terrorism, when special operations forces conduct an unacknowledged operation in a country where U.S. troops are not already present, how can they prove that it is in anticipation of involvement of the regular armed forces later on, and thus not a covert action that requires a presidential finding and congressional notification (particularly if it is "years in advance")?

An even more difficult question is, who will ask them to prove it? Legally, the ultimate arbiters of what does and does not constitute covert action would be the House and Senate intelligence committees, which exert a type of veto through their control of the intelligence authorization process. However, there are several problems with that argument. First, if it is a special operations mission, the funding would be controlled by the House and Senate Armed Services Committees, creating a crucial split between the authority to determine whether it is a covert action and budgetary control. Second, the Armed Services Committees have ultimate control over the intelligence authorization process in any case, because they must sign off on intelligence authorization bills before they go to the full House and Senate for a vote. As one Senate Armed Services Committee staffer described the relationship, "We prevail because they're subordinate to us." Finally, the fact of the matter is that congressional committees only know about those operations that the administration tells them about. They cannot ask questions about operations they do not know about.

Beyond the technicalities of arguing the meaning of the word *anticipated*, the Bush administration has made an even broader claim regarding its use of the military to conduct what would be called covert action if it were conducted by the CIA. Having defined the broad post-9/11 strategic situation as a "war on terror," administration officials argue that anything the government does to prosecute the fight against terrorism is part of a "war" and thus, legitimately a "traditional military activity." A variant of this argument stems from Senate Joint Resolution 23, the authorization to use force granted by the Congress in response to the September 11 attacks. That resolution authorizes the president "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons." Thus, according to some legal experts, the resolution grants the president virtually unlimited authority, as long as he "determines" that a particular target has some connection to Al Qaeda.

Finally, some Pentagon lawyers have interpreted the post-9/11 landscape even more broadly. Bush does not even need the resolution's authority, they contend; because of the attacks, anything he does in the fight against terrorism can be seen as a legitimate act of self-defense, and thus a "traditional military activity."

"SPECIAL ACTIVITIES"

Another aspect of the potentially increasing intersection of covert action and special operations forces, and its implications for congressional oversight, concerns whether the Pentagon is actually conducting covert operations but calling them something else. The Department of Defense has defined a category of so-called special activities with four characteristics. These are activities (1) that are conducted abroad; (2) in which the U.S. role is not apparent or acknowledged; (3) that do not include the collection or production of intelligence; and (4) that are not diplomatic activities. It is difficult to obtain precise information about such special activities, but they are conducted under some presidential authority, such as executive orders, and do entail some degree of congressional notification, although it is impossible to know how many and which members that includes. What is clear is that they are not conducted under the covert action requirements of the law and do not involve notification of whole committees, whether intelligence or armed services. The relevant question is, whatever they are called, are these operations subject to effective oversight?

Another overlapping category that includes unacknowledged operations is that of special access programs, or SAPs. SAPs, established by Executive Order 12958, are sensitive programs that impose "need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information." This "beyond top secret" designation is to be established only on an agency head's determination that (1) the vulnerability of or threat to specific information is exceptional, and (2) the normal criteria for determining eligibility for access are not deemed sufficient to protect the information.

The standard reporting requirement for SAPs is that the congressional defense committees be given thirty days' notice before the program is initiated. However, the Bush administration has effectively nullified this requirement since January 2002. In various executive orders and presidential signing statements accompanying defense legislation, Bush has included language claiming that the Supreme Court "has stated that the President's authority to classify and control access to information bearing on national security flows from the Constitution and does not depend upon a legislative grant of authority." As a result, he states that although in most situations the thirty-day advance notice can be provided, "as a matter of comity, situations may arise, especially in wartime, in which the President must promptly establish special access controls on classified national security information under his constitutional grants of the executive power and authority as Commander in Chief of the Armed Forces." The statements then make plain that the executive branch will interpret the reporting requirements "in a manner consistent with the constitutional authority of the President."

There are three categories of special access programs: (1) acknowledged programs, which are unclassified; (2) unacknowledged programs, which are classified but reported to Congress in the same form as acknowledged SAPs; and (3) waived programs, where the classifying agency head waives the standard

reporting requirement. Waived SAPs are only orally briefed to the so-called Gang of Eight, that is, the chair and ranking (minority) members of both the Senate and House intelligence (or Armed Services) committees, and the House and Senate Majority and Minority Leaders. The controversial program involving the National Security Agency (NSA)'s program of warrantless domestic surveillance that surfaced in late 2005 was one such waived SAP, apparently authorized by the CIA.

Army documents that came to light in early 2006 as a result of the ongoing Freedom of Information Act lawsuit brought by the American Civil Liberties Union against the Defense Department regarding the abuses at Abu Ghraib prison highlight the risks involved in special operations forces being both involved in the war on terror and covered by SAPs. These documents confirm that a special operations unit known as Task Force 6-26 (also known as Task Force Omaha) has been implicated in numerous detainee abuse incidents in Iraq. Moreover, one army file details how—because the unit was part of a SAP—an investigator was unable to continue an investigation into claims that a detainee captured by Task Force 6-26 in Tikrit, Iraq, was stripped, humiliated, and physically abused until he passed out.

There exists yet another process that provides for the protection of classified information. Known as Alternative or Compensatory Control Measures (ACCMs), these are a way of applying "need-to-know" restrictions on information to, in essence, compartmentalize a program. According to a Navy directive, ACCMs are to be used in situations where need-to-know restrictions are deemed necessary but SAP controls are not warranted. These measures are distinct from SAPs in that although they provide the same internal security standards, they do not need the formal approval of the agency head and they do not have to be reported to Congress. Since September 11, hundreds of ACCMs have been established to compartmentalize information regarding a range of sensitive activities, from special operations in specific countries to intelligence collection and processing programs to various war planning contingencies.

One indication of the potential for abuse of ACCMs came in an internal Navy audit conducted in 2005. The audit reportedly found that secrecy was being used to restrict congressional, Defense Department, and internal access to potentially controversial or even illegal activities. As a result of the audit's findings, the Navy's new directive on ACCMs states, "The use of ACCM measures shall not preclude, nor unnecessarily impede, Congressional, Office of the Secretary of Defense, or other appropriate oversight of programs, command functions, or operations."

There have been indications that some members of Congress are becoming uncomfortable with the Pentagon's increasing independence in the area of unacknowledged operations. In June 2005, the House Permanent Select Committee on Intelligence's report on the 2006 Intelligence Authorization Act stated the committee's belief "that it does not have full visibility over some defense intelligence programs" that fall outside of specific budget categories. Speaking to the press, Representative Peter Hoekstra (R-MI), the chair of the House committee,

expressed his concern that the Pentagon was trying to hide activities such as information operations programs, including electronic warfare, psychological operations, and counterpropaganda programs from both the newly created Director of National Intelligence and Congress.

Periodically, information about some previously unknown program will reach the public eye, and a few members of Congress will express their concern about whether the Pentagon is evading oversight restrictions. They often issue calls for hearings, which may or may not be held. Momentum for developing a more robust congressional oversight role of special operations, however, tends to be derailed by a combination of factors. Often, the Pentagon sends representatives to Capitol Hill for either closed-door briefings or closed hearings in which they explain how they are not violating the covert action restrictions because, by their own definition, they do not indulge in covert action (unless an individual operative is on assignment to the CIA). Rather, they explain, they are conducting special activities and they have complied with the relevant notification requirements (as interpreted by the administration).

Another factor working against congressional efforts for a larger role is the underlying antagonism between the intelligence and defense committees, and their respective sense of ownership of their particular issues. The concerns raised by today's special operations invariably involve both committees and will not be addressed adequately until this fundamental issue of turf sharing is resolved. Moreover, although members on both sides of the aisle have voiced concern, it has more frequently been expressed by the Democratic minority, which of course opens it up to partisan debate and power struggles, struggles the minority inevitably loses. Finally, members' motivation to increase their oversight role tends to wither in the face of Congress's traditional reluctance to go up against the Pentagon in a time of war.

ISSUES BEYOND CONGRESS

Another controversy regarding the expansion of special operations forces into the realm traditionally occupied by the CIA's covert operators involves the question of who is better suited to conduct such operations, whatever they are called. Pentagon officials contend that the CIA is not responsive enough to the military's needs, that it is too risk-averse, and that it is simply too small to meet the global terrorist challenge. The CIA has approximately 700–800 covert operators, compared to the roughly 10,000–13,000 special operations forces. On the other hand, their relative sizes are not as unbalanced as these numbers seem to indicate. Of that total, no more than 2,000 are JSOC black operators, that is, directly comparable to CIA operatives. Moreover, according to many analysts, the difference in size of the overall organizations is a significant advantage for CIA operators. Having much less bureaucracy to deal with, they can do things faster, cheaper, and with more flexibility than special operations forces—the

main reason, the CIA's advocates contend, that the agency was able to have men on the ground at the beginning of the Afghanistan war quicker than the military. Even though this has clearly been one of the Pentagon's priorities in enacting its SOCOM reforms, most analysts still believe that the CIA continues to retain an advantage in speed and flexibility.

The CIA also has the advantage of experience: It has been conducting this type of operation for a long time and thus has case officers stationed at embassies throughout the world who have built up an extensive network of contacts that the military simply does not have. In addition, conducting operations where the role of the United States is unacknowledged means, by definition, operating out of uniform. If captured, therefore, a special operations soldier is in an inherently different position than a conventional one. Whereas the latter is covered by international legal mechanisms such as the Geneva Conventions, which govern the conduct of war and the treatment of prisoners, a special operations soldier will have no such recourse. People who join the CIA's operations division are aware of and accept the risk that if captured, they will essentially be completely on their own and that their country will not acknowledge them. Soldiers, however, join with a different set of expectations. They generally assume that if they fight for and defend their country, Washington will do its best to protect them if they are captured. Although many special operations soldiers knowingly accept that risk, analysts point out that it is a dangerously slippery slope. Once some contingent of U.S. military personnel is left without protection, they argue, that endangers the protection of all military personnel serving abroad and could damage troop morale as well.

Many CIA and JSOC operators oppose the Pentagon's emphasis on moving special operations forces into the unacknowledged realm for precisely these reasons. There was, for instance, considerable opposition among special operations forces themselves to the 9/11 Commission's recommendation of moving all paramilitary responsibilities to SOCOM. Furthermore, these critics argue, JSOC's direct action units do not have the training for covert action operations, and if they do undertake the training required, that will detract from their readiness for their traditional, highly specialized missions, such as hostage rescue, close-quarters combat, and dealing with weapons of mass destruction. However, though there are other personnel capable of conducting covert action (i.e., in the CIA), if special operations forces are distracted from their traditional missions, there is no one else who can take their place, leaving the United States vulnerable in certain situations.

Critics of the Pentagon have also raised the concern that the military is running its own unacknowledged operations without notifying the "country team" (the CIA station chief and the ambassador) in the relevant location. Not only would this run the risk of embarrassing the United States diplomatically, but if the CIA were conducting an operation in the same area and the operators were unknown to each other, they could conceivably perceive each other as the enemy, a situation known as "confliction." In response to stories about such situations in the press in 2005, some members of Congress asked for an explanation from the

Pentagon. Defense Department officials testified that they had never conducted an operation without first notifying the country team, which allayed congressional concern. In addition, the Pentagon and CIA had various discussions regarding how to coordinate their operations better to avoid any risk of confliction.

Another question revolves around the actual difficulties in expanding special operations forces, particularly black operators. The Pentagon has called for a significant increase in special operations soldiers by 2011. However, the whole point of special operations forces is that they are the best of the best and are put through much more rigorous and thorough training than conventional soldiers. Many analysts have questioned SOCOM's ability to produce that many more operators, particularly when its training infrastructure is already under stress as a result of increased training loads ever since September 11. The command has revamped some of its training to make it more efficient and get more done in less time, but the fact remains that the high level of training for special operations requires a considerable amount of time, and many question whether the Pentagon's push for increased numbers will result in compromising the quality of the resulting forces.

One final issue that arises in weighing the differences between unacknowledged operations conducted by the CIA and by special forces stems from the differences in mission planning procedures between the two organizations. Traditionally, CIA covert operations are developed by an operational planning group and then subjected to several levels of approval within the Agency. After receiving the CIA's approval, the proposal is then reviewed by the deputies' committee at the National Security Council, and possibly by the principals themselves, before being passed on to the president. Military operational planning, however, is conducted quite differently. Because its primary mission is combat, the military has full authority to make its own operational decisions with no input from outside agencies. A military black operation, therefore, is planned completely within the Pentagon and approved by the secretary of defense. This insulated decision-making system raises obvious risks in a situation where special operations forces are conducting unacknowledged operations in a wide range of countries with which the U.S. has a variety of relationships.

COMMISSION RECOMMENDATIONS

In its final report, the 9/11 Commission stepped squarely into the debate over who is actually better suited to be leading the covert battle against terrorism. The commission recommended, "Lead responsibility for directing and executing paramilitary operations, whether clandestine or covert, should shift to the Defense Department. There it should be consolidated with the capabilities for training, direction, and execution of such operations already being developed in the Special Operations Command."[6] In response, President Bush asked the Pentagon and the CIA to study the commission's conclusion and come up with a joint recommendation. Although many assumed that because of the Pentagon's

political muscle and Rumsfeld's expressed goals, it was a foregone conclusion that the Pentagon-CIA study would agree with the commission's recommendation; in fact they ended up rejecting it, as did the President.

When the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Silberman-Robb Commission, after its chairs, Judge Laurence Silberman and former Senator Charles Robb) issued its recommendations in mid-2005, it reportedly included a classified recommendation that also would have given the Pentagon greater authority to conduct covert action. Once again, though, the White House rejected the recommendation. While this would seem to run counter to the Pentagon's moves to expand special operations in the years since 9/11, in the context of the definitional issues just explained, it appears likely that in fact the Pentagon does not want more control of covert action. It has the greatest freedom of action in the present system, whereby the CIA conducts covert action per se and is thus subject to more formal congressional oversight, whereas the Pentagon can continue conducting its special activities, SAPs and ACCMs, with minimal, sometimes nonexistent, oversight.

CONCLUSION

The question of the military's involvement in unacknowledged operations is shaped by four main factors. First is the Pentagon's broad vision of SOCOM's future role in the "long war" against terrorism. Second is the geographic expansion of special operations forces, in terms of the number of different countries in which both black and white operators are present. A third facet of the issue is the Pentagon's definition of unacknowledged operations as special activities, with more lenient congressional notification requirements than the covert action conducted by the CIA. In addition, the military has the special categories of SAPs and ACCMs that restrict information even further. Finally, there are the indications that some past SAPs have led to highly controversial policies, including renditions (the practice of seizing suspects in one country and delivering them into custody in another country), covert media influence operations in Iraq and Afghanistan, and the direct evidence of the involvement of Task Force 6-26 in interrogations at Abu Ghraib. The military's role in unacknowledged operations is an increasingly complex issue and it remains to be seen how Congress will serve the twin goals of protecting the United States from terrorism and ensuring that there is sufficient accountability to the public.

NOTES

1. 50 U.S.C. § 413(b)(e).

2. *Quadrennial Defense Review Report*, United States Department of Defense, 6 February 2006. Available at http://www.defenselink.mil/qdr/report/Report20060203.pdf

#search=%222006%20quadrennial%20defense%20review%22 (last accessed 24 August 2006).

3. Thom Shanker, "Pentagon Hones Its Strategy Against Terrorism," *New York Times* (February 5, 2006), p. 16.

4. 50 U.S.C. § 413(b)(e).

5. H.R. Conf. Rep. No. 166, 102nd Congress, 1st sess.; reprinted in *Congressional Record* 137, no. 115, H5904-06 (July 25, 1991), pp. 5905–6.

6. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W. W. Norton, 2004), p. 415.

BIBLIOGRAPHY

Cogan, Charles, "Hunters not Gatherers: Intelligence in the Twenty-First Century," *Intelligence and National Security* 19 (2004), pp. 304–21.

Fisher, Louis, *Presidential War Power* (Lawrence: University Press of Kansas, 1995).

Hammond, Jamie. "Special Operations Forces: Relevant, Ready and Precise," *Canadian Military Journal* (Autumn 2004), pp. 17–28.

Kibbe, Jennifer D., "The Rise of the Shadow Warriors," *Foreign Affairs* 83 (2004), pp. 102–15.

Marquis, Susan L., *Unconventional Warfare: Rebuilding U.S. Special Operations Forces* (Washington, DC: Brookings Institution Press, 1997).

Paddock, Alfred H. Jr., *U.S. Army Special Warfare: Its Origins* (Lawrence: University Press of Kansas, 2002).

Reisman, Michael W. 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).

Robinson, Linda, *Masters of Chaos: The Secret History of the Special Forces* (New York: Public Affairs, 2004).

Stone, Kathryn, *"All Necessary Means"—Employing CIA Operatives in a Warfighting Role Alongside Special Operations Forces* (Carlisle Barracks, PA: U.S. Army War College Strategy Research Project, 2003).

8

COVERT ACTION AND DIPLOMACY

JOHN D. STEMPEL

COVERT ACTION AND DIPLOMACY HAVE HAD A long and checkered career together for over two millennia. From the earliest organized governments, when functions were not sufficiently differentiated, clandestine operations were standard practice in international relations. Beginning with the Achaemenid Persians between the sixth and fourth centuries B.C., the organization of intelligence as part of government was developed to a very high degree and copied by Arabs, Turks, Afghans, Mongols, and Hindus over the following centuries. Activities that we now consider covert action—assassination, coopting the king's counselor (or mistress), paramilitary support for insurgencies, and propaganda—were common. There was little or no distinction between "intelligence" and "covert action" until the nineteenth and twentieth centuries. That developed in the West as a result of the evolution of Westphalian diplomacy in the fifteenth and sixteenth centuries.[1]

The emergence of Western diplomacy was driven by the disastrous desolation caused by the Thirty Years' War. Crude but temporary diplomatic missions began in the fifteenth century in Venice and the Italian states and spread to Europe. Intelligence and eventually secret operations were an integral part of these activities, though they were fairly simple by modern standards. In the Elizabethan period, British covert action multiplied the effective power of England, especially when the use of gold and Protestant mercenaries as diplomatic weapons saved the Protestant cause in France and the Low Countries.

By end of the Napoleonic Wars in 1815, the Treaty of Vienna included the regulation of diplomatic ranks and began the formal organization of diplomacy under international laws regulating diplomatic rights and duties. It included the principles that diplomats are not to interfere in the internal affairs of states and an outright condemnation of espionage.[2] Of course, this did not stop spying, but it

forced intelligence services to become more professional and began the differentiation between intelligence and diplomacy in terms of norms, objectives, and means and methods.

As other European societies followed Britain through the Industrial Revolution, and as continental European politics became more complex through the eighteenth and nineteenth centuries, intelligence services and capabilities grew. The United States entered the diplomatic arena in the late eighteenth century after winning its independence from Britain, but distance, communications, and time kept it from playing a serious role in European and world politics until nearly a century later. The 1898 Spanish-American War, coupled with World War I brought the United States into the world arena.

Because of this history, America lagged behind the rest of the world in developing an organized intelligence capability. Throughout most of the nineteenth and early twentieth centuries, both U.S. intelligence and diplomacy were ad hoc affairs, which included secret operations on occasion, where needed and possible. Roosevelt's maneuvers involving the acquisition of the Panama Canal are a good example. In fact, the United States had no professional diplomatic community until the Rogers Act of 1924, and until 1940, no formal intelligence organizations existed except the military service intelligence departments.

George Washington created his own informal intelligence network during the American Revolution, but it dissolved after the American victory at Yorktown. The U.S. Army began to develop intelligence units during and after the Civil War experiment with outsourcing intelligence to Allan Pinkerton's organization. Formal organizations were not created until the 1880s in the Army and Navy Departments.[3]

In World War I, the military services ran their own shows, and a civilian Committee on Public Information under George Creel focused largely on propaganda and internal security. During the interwar years (1919–39), American intelligence lapsed back into previous peacetime routines, with the military service units dominating the field. American code-breaking efforts were terminated in 1929.

As the war clouds grew over Europe again in the late 1930s, President Franklin Roosevelt selected William O. Donovan to create the Office of the Coordinator of Information in June 1941, which became the Office of Strategic Services (OSS) the next year. This was the first organized American effort to conduct what became know within the next decade as covert activities—propaganda, political operations, economic operations, and paramilitary activities, as well as sabotage, espionage, and counterespionage during World War II.

When the OSS was disbanded in September 1945, President Truman transferred its intelligence functions to the State Department, where they became the Bureau of Intelligence and Research. He also created the Central Intelligence Group (CIG) a year later to keep the rest of the trained professionals, including covet action operators, together until the United States could sort out its postwar needs.[4]

Most of today's scholarly work cites the creation of the Central Intelligence Agency (CIA) in 1947 as part of the National Security Act as the real beginning of professionalized intelligence in American government.[5] The vast increase in technological capabilities—such as better communications and space photography—required a much greater concentration of resources and manpower to succeed. Cooperation with Allied intelligence services in World War II socialized Americans to international intelligence work. The imperatives of postwar politics and the rise of the Cold War made such an effort necessary on a continuing basis.[6]

The CIA has maintained its links with the State Department and the military in Washington. Abroad, U.S. and other countries' embassies often host resident personnel under "official" cover. However, the overall tension between the utility of covert action and the requirements of diplomacy and foreign policy continue to this day, breaking out in open hostility on occasion.

COVERT ACTION: METHODS AND OPERATIONS

Covert action is formally referred to in presidential executive orders as "special activities." Perhaps the most inclusive general description is Jeff Richelson's: "Covert action, also known as "special activities," includes any operation designed to influence foreign governments, persons, or events in support of the sponsoring government' s foreign policy objectives while keeping the sponsoring government's support of the operation secret. Whereas in clandestine collection, the emphasis is on keeping the activity secret, in covert action the emphasis is on keeping the sponsorship secret."[7] Such activities are aimed at keeping the sponsoring government's role secret, but they also do violate the diplomatic Vienna Convention injunctions against interference in the domestic affairs of the host country.

When a covert action is uncovered, the sponsoring country's relations with the target country are adversely affected. This generally brings diplomats back into the problem, because they are the ones who take the brunt of criticism and later raise the general foreign policy question of whether such actions were or are worth the cost. Before pursuing this discussion, the following section examines the types of actions and individual issues/problems. Although much is known about historical operations, details on present-day activities are scarce. This circumstance hampers a complete and fully informed discussion.

Propaganda, sometimes called psychological warfare, or psy ops, has both overt and covert aspects. The press and cultural sections of embassies pass out overt, or "white" information that is attributed to official sources and represents the government's official view. "Gray," or partially concealed propaganda and "black" propaganda that are attributed to someone else, such as falsified statements from a foreign government, are concealed variants. All these types of propaganda were used to influence the 1948 elections in Greece and Italy against the

communists. The Soviets made heavy use of all three types from 1945 to the demise of the Soviet Union.[8] Other countries consistently use white propaganda (e.g., the British Broadcasting Company and the French Press Agency).

Examples of black operations include the American establishment of a clandestine radio station in Guatemala that broadcast news of a revolutionary army so convincingly that the procommunist president resigned. Soviet efforts to convince Africans that the United States was responsible for creating AIDS are similar black efforts. A similar clandestine operation publicized in late 2005 told of U.S. military officials paying to have stories placed in the Iraqi press lauding the role of American soldiers in trying to enhance security in Iraq.

For many years, Radio Free Europe and Radio Free Liberty dispensed gray information while covertly supported by the CIA as privately supported organizations. In 1973, Congress gave them independent status under the Board for International Broadcasting to "whiten" their offerings. Such activities are estimated to constitute about 40 percent of the CIA's covert activities.

Economic operations have been the least used covert activities by the CIA, accounting for only 10 percent of U.S. covert activities. Economic support in terms of goods shipments to support friendly governments or withholding trade with unfriendly countries occurs on both the overt and covert levels. Sanctions are overt; manipulating a national currency clandestinely is covert. Much of the action against the Allende government in Chile in the early 1970s involved economic issues, including inciting labor strikes and depressing the world copper price. Positive efforts include measures to restore Iraq's economy after the American defeat of Saddam Hussein in 2003 and shipments of food to friendly countries under the Public Law (PL) 480 program. Economic measures are often overt as well as covert, and these include foreign aid as well as favorable trade pacts. Efforts to beef up the cattle and food industries in Africa are normally overt, but given sensitivities in some areas to the HIV/AIDS problem, covert measures to give additional vaccines and medicines to people in certain places may be necessary.

Political action is a more diffuse and complex category, involving everything from financial support for key leaders to creating insurgencies. Such action accounts for about 30 percent of U.S. covert activities. Some known examples include payments to Jordan's King Hussein, giving money and campaign advice to the Solidarity movement in Poland in the 1980s, and supplying political organizational personnel and money to Afghan politicians since 2002.

In addition to major U.S. efforts in Western Europe in the 1940s, there were two campaigns in Chile in 1964 and 1970. The first was a solid success; the second failed to prevent Salvadore Allende from becoming president and led to a campaign to overthrow him that was a major trigger for the Church Commission's 1974–75 investigation of the CIA.

Moving toward activities that present an even greater challenge to international norms, there are instances where both the United States and the Soviets Union supported coupes d'etat against foreign leaders. Soviet support for coups

in Czechoslovakia in 1948 and in Afghanistan 1n 1978 are clear-cut cases of the exercise of Soviet political and eventually military power. The Soviets supplied political support to a number of other regimes including Cuba, Angola, Iraq, and Mozambique up to and including use of force over the past 60 years.

The U.S. has been identified with four other coups in addition to the Guatemalan and Chilean examples given. In 1953, some money and organizational skills were supplied to forces loyal to the shah, which brought down Prime Minister Mossadeq's government and restored the monarchy. The overthrow of the shah twenty-five years later drew substantially on Iranian anger at the earlier effort and raised the question of whether the 1953 coup was effective in protecting long-term U.S. interests. Successful U.S. efforts in 1961 to oust Trujillo from the Dominican Republic and acquiescence in an army coup that killed South Vietnamese President Ngo Dinh Diem in 1963 are other cases the Church Commission discussed.The United States also gave political support to those seeking to oust Philippines President Ferdinand Marcos in 1986 and political and active military support to oust the regime in Grenada in 1983, Panamanian President Manuel Noriega in 1989, and the Haitian military dictatorship in 1993–94.

Paramilitary activities, including assassinations, often overlap with or are carried out in conjunction with political action operations. They generally involve more risk and controversy than any other type of covert action. The CIA's Special Operations Unit ran a "secret" war against the North Vietnamese puppet regime in Laos from 1963 until the United States withdrew from Vietnam in 1973. CIA support for other wars/guerilla operations has included action in twenty-six publicly identified countries, including the Ukraine, Poland, Albania, Hungary, Indonesia, China, Oman, Malaysia, North Korea, Venezuela, the Dominican Republic, Bolivia, Guatemala, Cuba, Nicaragua, El Salvador, Angola, Greece, Afghanistan, and Iraq. Soviet operations include at least that many countries over the seventy-two years of the regime's existence.

Some clandestine American activities involved support for or protection of other elements of the clandestine intelligence collection process, including the maintenance in Iran of monitoring stations to track Soviet missile launches and monitoring sites in Laos and Cambodia for following North Vietnamese troop movements. In the 1980s, American covert operations involving Pakistani aid to the Afghan rebels against the Soviet puppet regime there were major factors in the eventual Soviet withdrawal in 1989. As in most other large-scale operations, part of the activity was covert, the rest merely secret, much of which eventually became public.

THE NEW TERRORISM

One of the spillovers from American Afghan operations in the 1980s and the Gulf War of 1990–91 was the rise of Islamic terrorism, which eventually led to the destruction of the World Trade Center towers and damage to the Pentagon on

September 11, 2001, when Al Qaeda–trained terrorists flew aircraft into these buildings. Subsequent military action in Afghanistan that destroyed Taliban rule there and chased Al Qaeda into Pakistan was greatly facilitated by both overt and covert operations that relied heavily on CIA cooperation with U.S. military forces, and paramilitary efforts were key to early success. Coordination between the CIA and Defense Department forces, however, did not remain uniformly good throughout and remains a subject of concern to intelligence reformers.[9] Failure to destroy or capture a significant number of Al Qaeda forces and leaders was one of the issues that led to the 9/11 hearings and intelligence reform in 2004–5. A related issue was the use of intelligence in the decision to attack Iraq in March 2003. The misreading of Iraqi nuclear and chemical/biological capabilities and the limited American understanding of Iraq and its politics brought forth criticism on both counts.

The concentration on intelligence reform led to a reassessment of American intelligence capabilities and a reorganization of the intelligence community under a new Director of National Intelligence (DNI).[10] Although the most intense focus centered on the more strenuous overt and secret activities, covert action has been affected as well. Information now available suggests there is more increased covert activity in support of penetrating terrorist cells and infrastructures. Support activities related to U.S. invasion and occupation of Iraq, and U.S. support of Afghanistan's democratic experiment post-2001, have grown dramatically. In these areas, paramilitary operations and support are crucial, overt or covert. This concentration suggests there are fewer resources for and less reliance on covert activities elsewhere, but this is speculative at this time (2006).[11]

COVERT ACTION: ASSESSMENT

As covert action became a bureaucratized activity in U.S. foreign policy after World War II, rather than an ad hoc political or military event, it became controversial. For over twenty-five years after 1945, during the Cold war, Americans treated covert activities with a "don't ask, don't tell" mentality. This followed a familiar pattern: most nations do not now and never have openly discussed their covert activities. There have been some academic discussions of past efforts when material became available or when enterprising journalists uncovered unsuspected connections. However, these tended to be one-shot stories with little follow-up. This began to change in the United States in the early 1970s when U.S. involvement in Chile drew the attention of Senator Frank Church and others. In 1975–76 a congressional commission investigated alleged intelligence abuses.[12] The Church Commission and subsequent government and scholarly efforts have focused on three issues: Is covert action effective? Is covert action under control? Is covert action moral?

Literature on effectiveness from both academic and professional sources stresses several negative points:

1. The "blowback" from failed operations—or even successful ones—damages U.S. foreign policy.
2. Americans are deficient in the cultural understanding necessary to successfully manipulate other cultures, hence covert action often ends badly.
3. Covert action is not an effective mechanism for resolving crises and has to be integrated as part of an effective policy to succeed.
4. Often, the objectives of the covert activity are not compatible with American values.
5. Often, unclear boundaries between covert action and military operations result in failures.
6. Short-term successes often lead to long-term disasters.[13]

Others, including some critics, concede that despite difficulties, covert action is something that can be useful if it is used properly: (1) if covert activities are integrated into coherent overall foreign policy; (2) if active coordination is maintained between all government agencies; and (3) if no overt options will accomplish the mission. Most agree that other options should be exhausted—much of the political and propaganda work should be done openly, and it must be done competently with a good chance of success. Like other choices for effective action, there are pitfalls as well as possibilities.[14]

The dispute over effectiveness spills over to the second issue: Is covert action under proper control? For Americans, this means conforming to relevant legislation and final presidential approval of such action. President Reagan's definition of covert action, published in Executive Order 12333 in 1981 and still in effect today, covers "special activities conducted in support of national foreign policy objects abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly . . . but which are not intended to influence United States political processes, public opinion, policies, or media and *do not include diplomatic activities or the collection or production of intelligence and related support functions*" (emphasis added).[15]

The U.S. Congress found this definition acceptable and incorporated similar language in its 1991 Intelligence Authorization Act. The common theme was that covert action is *not* an intelligence activity, and the requirements for a presidential finding did not apply to diplomatic activities. Also, such special activities were not to be targeted at or designed to influence the American public or American politics.

The development of a working definition of *covert action* stemmed from the work of the Church Commission, which at first called the CIA a "rogue elephant," but then backed away from that view in its final report. No other country deals with covert action this way. In 1994, the Hughes-Ryan legislation, which required the presidential finding for covert action, also ended the doctrine of plausible denialability for the president.

The presidential finding combines a determination that the activity is important enough to U.S. national security that it should be undertaken despite the risks and

possible exposure, and that the purpose for which it is undertaken and the methods used would be approved should it become public—the risk should be worth it. In 1986, the Iran-*contra* scandal underscored the reason for such legislation when it broke. National Security Council officials John Poindexter and Oliver North concocted a scheme to sell weapons to Iran in return for the release of American captives in Beirut and then (illegally) use the proceeds to fund U.S. operations against the Nicaraguan Sandinista government by supporting the contras.

This operation was never a true covert action, because approval was never sought. Some CIA, diplomatic, and military officials were involved in these basically criminal activities that were kept from Congress's attention until the story was revealed abroad. A few were tried in court, others were fired, and some left government voluntarily. There was considerable anger among the professionals in the various agencies. President Reagan escaped serious censure when he apologized to the country in a televised speech following the scandal.[16]

Journalists and students of intelligence had a field day with the Church Commission's initial allegations about rogue elephants and with the Iran-*contra* scandal, as they often do when intelligence operations go awry.[17] Ever since the 1960s, periodic book and magazine exposés have vied with serious analysis for public attention when covert action is the subject. This highlights the continuing tension between the secrecy needed for covert action and intelligence activities and the requirements for democratic transparency in government. A few other democracies have begun to gently question intelligence activities, but in most nations this is a nonproblem—these matters are simply not discussed.

The final question is whether covert action is moral. It is always justified as important or even vital for national security. It has been separated from diplomacy and discouraged in international law because it is not considered an acceptable part of international relations. Nevertheless, it persists—as do efforts to codify and extend international law.

Throughout the Cold War, America operated on the basis of the view developed by a panel appointed by President Eisenhower. Headed by retired Gen. Jimmy Doolittle, its report said that in view of communism's win-at-all-costs approach to foreign affairs, the United States would have to reconsider its concepts of fair play and undertake to subvert, sabotage, and destroy our enemies.[18] America did not fully trade morals for realpolitik, but it certainly erred on the side of a more vigorous covert action policy.

Beginning with the Carter administration and reemerging with the Clinton administration, the question of how moral our foreign policy was continued to bubble. The Reagan administration returned to the more forceful arguments for fewer limits on covert action, and so did the first President Bush; after 9/11, so did President George W. Bush. Key players in his administration consistently made the argument that the brutality and viciousness of the terrorists required the utmost response. However, the president's policy of bringing democracy to the Middle East, which justified the 2003 invasion of Iraq, also raised the question of

whether covert actions by their very nature undercut strategies to promote democracy in Iraq and elsewhere.[19]

Several writers have made the argument that covert action must be considered in terms of just war theory and that covert action can be justified in some circumstances, but it should not be used as a "lazy country's way of avoiding hard diplomatic work."[20] Some former agents argue that collecting intelligence and covert action often involve working with amoral characters, especially when terrorists such as Al Qaeda are the targets.[21]

They have a point, and no one has said the choices are easy. Most thoughtful writers suggest that some form of the following guidelines would give a government a solid base for defending covert actions if they went bad, and that most people would support covert action taken for the following reasons:

1. The president approves the covert action after organized deliberation within the executive branch and the legally required consultation with Congress.
2. The action's intentions and objectives are clear, reasonable, and just and are also part of a coherent foreign policy.
3. Overt means of advancing the policy will not work.
4. There is significant probability of success, with minimal damage to innocent people.
5. Damage inflicted should be proportional to the threat reduced or averted.

Of course, such assessments have and could turn out to be wrong, or actions could be botched or turn out badly. There is really no way of averting criticism or political damage, but a defense of just covert action will limit damage to the diplomacy of the country that can so defend itself politically if matters go badly.

Using such guidelines may also assist in minimizing organizational struggles and clashes within the intelligence, defense, and diplomatic communities. If all work from the same page, intragovernmental spats will be minimized because positions will have to be harmonized or adjusted before action can get under way. Legal issues would be minimized, and there will also be more markers for judging the effectiveness of covert action. Those who have put themselves above the requirements for control are those who caused real damage to the system. They have also raised the bar of distrust across both international as well as domestic dimensions.

CONCLUSION: THE FUTURE

Combining considerations of effectiveness, control, and morality has and will help governments assess and carry out special activities in a future that is coming at us with dizzying speed.

When the United States began its romance with covert action in the late 1940s and '50s, leaders of developing new nations had not yet mobilized masses of people in the developing world for political action. Politics was still very much an elite game when Kermit Roosevelt helped restore the shah to power in 1953. The mobilization of Iran's Islamic population by Khomeini and others made covert action almost impossible. The OSS successes in France and Burma during World War II were difficult to repeat in the Eastern Europe of the 1940s and '50s. Similarly, the triumph of mass movements in other African and Middle Eastern states in the 1960s increased the need for effective diplomacy while simultaneously reducing the productive scope of covert activities.

Similarly today, the explosion of cell phones, computers, and the Internet has complicated covert operations. The geometric increase in surveillance capacities and means for harming others has both helped and hindered cover actions, and foreign policy and intelligence become more complex and interlinked than they have ever been.

The result, certainly for the United States, had been a reassessment of intelligence and the creation of a new Director of National Intelligence. Covert action has come under renewed scrutiny. Paramilitary efforts were stepped up in the wake of 9/11. Efforts have been made to increase public diplomacy and bring politics activities into more transparent light.

All postwar presidents have used covert action with congressional approval since 1974 (the exceptions have resulted in disgrace and/or punishment for the culprits). It is not unreasonable to suggest that they will continue to do so in a dangerous world. To achieve success, however, they will have to keep in mind the pitfalls and problems connected with such activities, as well as the guidelines for success listed above.

Ultimately, all connected with such activities need to bear in mind the words of former National Security Agency Director William E. Odom: "Intelligence performance simply can not be separated from foreign policy making and military operations."[22]

NOTES

1. For history on these points, see Keith Hamilton and Richard Langhorn, *The Practice of Diplomacy* (New York: Routledge, 1995); G. R. Berridge, *Diplomacy: Theory and Practice*, 3rd ed. (New York: Palgrave, 2002); and Adda Bozeman, *Strategic Intelligence and Statecraft* (Washington: Brassey's, 1992).

2. Berridge, *Diplomacy*, pp. 618ff.; for more detail see Garrett Mattingly, *Renaissance Diplomacy* (New York: Houghton Mifflin, 1995).

3. See Scott Breckinridge, *The CIA and the U.S. Intelligence System* (Boulder, CO: Westview Press, 1986), chap. 1: Jeff Richelson, *The U.S. Intelligence Community* (Boulder, CO: Westview Press, 1995), chap. 1.

4. Charles D. Ameringer, *U.S. Foreign Intelligence: The Secret Side of American History* (Lexington: Lexington Books, 1990). This is an excellent and readable, swift

review of U.S. intelligence from the country's inception through the Reagan administration, including covert action.

5. Richelson, *Intelligence Community*; Rhodri Jeffreys-Jones, *The CIA and American Democracy* (New Haven, CT: Yale University Press, 1989), intro and chaps. 1, 2; Abram N. Shulsky, *Silent Warfare: Understanding the World of Intelligence* (Washington: Brassey's, 1991), chaps. 2 and 14.

6. Breckinridge, *CIA and U.S. Intelligence*, part 1.

7. Richelson, *Intelligence Community*, p. 3.

8. Christopher Andrews and Vasili Mitrokhin, *The World Was Going Our Way: The KGB and the Battle for the Third World* (New York: Basic Books, 2005), is an excellent review of Soviet activities.

9. Sean Naylor, *Not a Good Day to Die* (New York: Berkley Books, 2005); William E. Odom, *Fixing Intelligence* (New Haven, CT: Yale University Press, 2003), chap. 4 and conclusion.

10. Steve Strasser, ed., *The 9/11 Investigations: Staff Reports of the 9/11 Commission* (New York: Public Affairs, 2004).

11. Paul Pillar, *Terrorism and Foreign Policy* (Washington: Brookings Institution, 2001); Strasser, *9/11 Investigations*; Odom, *Fixing Intelligence*, pp. 150–92.

12. Breckinridge, *CIA and U.S. Intelligence*, parts 2 and 3; Loch K. Johnson, *America's Secret Power: The CIA in a Democratic Society* (New York: Oxford University Press, 1989); Loch K. Johnson and James J. Wirtz, eds., *Strategic Intelligence: Windows into a Secret World* (Los Angeles: Roxbury, 2004), part 8.

13. Excellent examples and discussions of these points may be found in William J. Daugherty, *Executive Secrets: Covert Action and the Presidency* (Lexington: University Press of Kentucky, 2004), chaps. 1–3; Chalmers Johnson, *The Sorrows of Empire* (New York: Metropolitan Books, 2004); Anonymous [Michael Sheuer], *Imperial Hubris: Why the West Os Losing the War on Terror* (Washington: Brassey's, 2004); Michael Sheuer, *Through Our Enemies' Eyes* (Washington: Brassey's, 2002); Odom, *Fixing Intelligence*, chaps. 7 and 9; Johnson, *America's Secret Power*, chaps. 6–9; Kim Roosevelt, *Countercoup: The Struggle for Control of Iran* (New York: McGraw-Hill, 1979); Stephen Kinser, *All the Shah's Men* (Hoboken, NJ: Wiley, 2003); Naylor, *Not a Good Day to Die*. Of these authors, four are former intelligence professionals, two are academics, and two are journalists.

14. Daugherty, *Executive Secrets*, conclusion; Odom, *Fixing Intelligence*, chaps. 7–9; Johnson and Wirtz, *Strategic Intelligence*, chaps 17, 19, 21, 28.

15. Executive Order 12333, U.S. Intelligence Activities, December 4, 1981, 3 CFR 200 (1981, 46 FR 59955, as amended by Executive Order 12701, 14 February, 1990, 55 FR 59333).

16. Daugherty, *Executive Secrets*, pp. 34–37; Bob Woodward, *Veil: The Secret Wars of the CIA, 1981–1987* (Buccaneer Press, 1994). 17. David Atlee Phillips, *The Night Watch* (New York: Ballantine Books, 1982); Victor Marchetti and John Marks, *The CIA and the Cult of Intelligence* (New York: Knopf, 1974).

18. Johnson and Wirtz, *Strategic Intelligence*, chap. 22.

19. David Rieff, *At the Point of a Gun: Democratic Dreams and Armed Intervention* (New York: Simon and Schuster, 2005), pp. 173–76; Stephen M. Walt, *Taming American Power: The Global Response to U.S. Primacy* (New York: Norton, 2005), pp. 243–47.

20. The source of the quote is a former intelligence officer who also served with the Foreign Service. The same themes can be found in Johnson, *America's Secret Power*, pp. 261–62; Daugherty, *Executive Secrets*, pp. 67–70 and conclusion; Johnson and Wirtz, *Strategic Intelligence* 278–79.

21. Robert Baer, *See No Evil* (New York: Crown, 2002); James Risen, *State of War* (New York: Free Press, 2006).

22. Odom, *Fixing Intelligence*, p. 186. Robert W. Pringle Jr. and Jennifer Griffin aided the author in identifying several sources.

9

FROM COLD WAR TO LONG WAR

Covert Action in U.S. Legal Context

JAMES E. BAKER

INTRODUCTION

ALTHOUGH COVERT ACTION HAS HISTORICALLY PLAYED A small part in the overall intelligence budget, as an intelligence function it has played a disproportionately large role in defining public perceptions of "intelligence,"[1] shaping congressional oversight, and policy impact. This reflects the reality that covert activities bear particular policy and legal risks as well as benefits. Covert action has historically included activities on a continuum between diplomacy and acts of war undertaken to hide the national footprint.[2] As a result, these activities are undertaken without the ordinary mechanisms of policy preview and external validation. Thus, although the law pertaining to covert action permits and prohibits, most of all it regulates its use by creating substantive thresholds triggering statutory and executive processes for authorizing and then appraising covert activities. These processes are intended to ensure that the means to effect covert actions are lawful, but also that the policy choices are sound and effective and that the gain from action exceeds the pain, in both the short and long run.

This chapter is divided into two sections. The first places covert action in contemporary policy and legal context. In a global low-intensity conflict against nonstate actors intent on conducting acts of terrorism with high-intensity consequences, clandestine activities of the sort historically identified as covert action play a central role. However, because this conflict is fought over values, including legal values, and because success in this conflict requires intelligence alliance, the when, why, where, and how of covert action takes on added importance. Contemporary law provides a procedural framework for addressing these issues within a context of limited access.

The second section raises three legal policy issues: (1) Will the president's wartime authority as commander-in-chief eclipse or marginalize the statutory framework for addressing covert action? (2) Does the statutory definition of *covert action* remain viable in light of the evolving use of "liaison" and "traditional activities" to combat terrorism? (3) Is the measure of executive preview and review adequate to address the policy and legal risks inherent in covert action, as well as those contemporary activities that bear comparable policy and legal risks?

LEGAL FRAMEWORK: A THUMBNAIL SKETCH

American covert action predates the Republic. Benjamin Franklin, the colonial envoy in France employed tradecraft like secret writing and dead drops to organize an espionage ring in Paris. Notably for this chapter, he also engaged in the covert planting of disinformation in the Paris press and the clandestine shipment of arms to the Colonies.[3] Covert action has been one of America's national security tools ever since. During the Cold War the United States (and the Soviet Union) engaged in a number of "overt-covert actions," such as the landings at the Bay of Pigs, the supply of the *contras*, and provision of support to the Afghan *mujahedeen*. Such "covert" mechanisms allowed proxies to engage in hot war, while the great power conflict remained "cold." (However, most covert activities, then and now, are secret and remain so.) Resort to covert action also reflected the strategic view that the threat posed by communism warranted resort to all the instruments of national policy.[4]

In a conflict against Islamic Jihadists, the United States should be expected to use all the national security tools, including covert action. Indeed, the instrument is well suited to address a nonstate opponent, acting outside the laws of armed conflict and operating without necessity of a particular territory, base, or even chain of command. In theory and in law, covert action is fast and flexible, allowing prompt response or proactive use against a mobile opponent within states either unwilling or unable to effect their capture. And in theory and in law, covert action is nonattributable and secret. This allows assisting states to otherwise deny complicity in necessary but locally unpopular actions. It also removes the "made in America" label, where for example, an audience might otherwise be receptive to the message, but not the messenger. For these reasons the law related to the authorization and review of covert activity is on the front line of counterterrorism. For these same reasons, the law, process, and practice of covert action will surely evolve from Cold War to "Long War" understandings and applications.

Constitutional Context

The president's inherent intelligence powers are found in enumerated constitutional authorities over foreign affairs and national defense as recognized in long-standing executive practice as well as in those few Supreme Court decisions

that address intelligence.[5] The extent to which the president's inherent authority is magnified as commander-in-chief in time of conflict is a matter of debate, in the intelligence as well as military spheres of security. However, there is surely a wartime gloss that attaches to exercise of executive authority during conflict overseas, but wider debate on whether or how such a gloss applies at home.

Congress's authority over the intelligence function is found in the funding power, the "necessary and proper" clause, its general legislative power, as well as the range of enumerated authorities the Congress possesses over national defense. The law provides for congressional notification of covert action and not consultation or approval, a constitutional acknowledgment of the president's particular authority in this area. However, in constitutional practice, strong legislative resistance can shape or even lead to the termination of a covert action program. Congress's leverage increases when a program requires the authorization and appropriation of new money (as opposed to presidential authorization to spend existing funds) or where Congress chooses to use the power of the purse to "fence" funding.

Statutory Context

Although there are a number of statutes that address intelligence, the National Security Act of 1947, as amended, remains the bedrock of U.S. intelligence laws. This is true in the area of covert activity. The act, in some manner or another, has served as statutory authorization for covert activity since 1947;[6] however, it was not until 1990, in the wake of the Iran-*contra* affair, that the Congress defined covert action in law. "DEFINITION: Covert Action is defined by what it is, an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[7] Through negative definition, "Covert action . . . does not include—(1) activities the primary purpose of which is to acquire intelligence or traditional counterintelligence activities; (2) traditional diplomatic or military activities or routine support to such activities; (3) traditional law enforcement activities; or, (4) activities to provide routine support to overt U.S. activities abroad."[8]

This definition was intended to capture activities that Congress determined should be channeled through a particularized process of executive authorization and congressional notification because of the nature of and risk inherent to the activities involved. The definition was meant to reflect existing practice, the legislative history stating: "It is not intended that the new definition exclude activities which were heretofore understood to be covert actions, nor to include activities not heretofore understood to be covert actions."[9] As a result, historical practice is particularly relevant to legal interpretation, albeit hard to ascertain using ordinary methods of legal research. The legislative history as well is particularly important in fleshing out the meaning of "traditional" activities exempt from the definition's reach.

Notably, this definition is act-based, not actor-based. This means that the law applies not just to the Central Intelligence Agency (CIA) but also to the Department of Defense and the Federal Bureau of Investigation (FBI) and other government entities, *provided* the contemplated activity fits the positive definition of covert action and is not otherwise "traditional." However, identity *is* relevant in determining whether an activity is traditional. For example, certain activities like raids might be traditional if undertaken by military actors in uniform during armed conflict; however, the same result may not follow if the raid were undertaken by nonattributable U.S. surrogates in peacetime. Of course, activities that were "extraordinary" before September 11, 2001, may have become ordinary and traditional since then.

FINDINGS

The act also recognizes the president's direct responsibility for covert action. The president is required to find that "an action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States."[10] Findings must be in writing, "unless immediate action by the United States is required," in which case a contemporaneous notation of the president's decision shall be made and a written finding produced within forty-eight hours. Reflecting some of the issues identified in the Iran-*contra* context, findings must also specify the department or agencies authorized to fund or participate "in any significant way" in an action, as well as specify whether the participation of third parties (e.g., third countries or persons) is contemplated.[11]

REPORTING

The act also requires the president to ensure that findings are reported to the intelligence committees "as soon as possible after . . . approval and before initiation."[12] The ordinary process of notification is in writing to the full committees. In practice, this means not only to the members but also designated staff with an oral briefing accompanying the underlying document. However, "To meet extraordinary circumstances affecting vital interests of the United States,"[13] the president may limit notification to the so-called Gang of Eight (the chairs and vice chairs of the Intelligence Committees and the Majority and Minority Leaders of each house of Congress) "and such other member or members of the congressional leadership as may be included by the President." Exercise of this option requires a statement from the president indicating why the action in question warrants limited notification. It follows that a limited notification is to members only and may be done orally. The president may, of course, authorize notification to additional members of Congress, or staff, something in between the full committee and the Gang of Eight. Although there may be good tactical reasons to do so, as in the case of members serving on the Appropriations Committees, selective

notification to preferred members of Congress or staff would seem to erode the premise behind limited notification.

Finally, the act implicitly authorizes the president to withhold notification altogether by stating that "whenever a finding is not reported [in one of the first two manners], the President shall fully inform the intelligence committees in a timely fashion and shall provide a statement of the reasons."[14] There is no public indication of whether this provision has ever been invoked.

In addition to reporting findings, significant changes to or significant undertakings pursuant to a previously approved action must be reported "in the same manner as findings are reported." This language is implemented through presidential Memoranda of Notification (MONs), which supplement, amend, or clarify previously approved findings. It follows that MONs are reported to the Congress using one of the three mechanisms specified for reporting findings. The triggering threshold for significant undertakings or changes has been the subject of internal executive debate as well as debate in Congress. The legislative history gives two examples. First, "this would occur when the President authorizes a change in the scope of a previously approved finding to authorize additional activities to occur. The second type of change specified in this subsection pertains to significant undertakings pursuant to a previously approved finding. This would occur when the President authorizes a significant activity under a previously-approved finding without changing the scope of the finding concerned."[15] These same terms were addressed in National Security Decision Directive 286, signed by President Reagan in the wake of Iran-*contra*, stating: "In the event of any proposal to change substantially the means of implementation of, or the level of resources, assets, or activity under, a Finding; or in the event of any significant change in the operational condition, country or countries significantly engaged, or risks associated with a special activity, a written Memorandum of Notification (MON) shall be submitted to the President for his approval."[16]

Finally, the act requires the president to "ensure that the Intelligence Committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this Title."[17] Likewise, Section 503 of the title pertaining to covert action requires the Director of National Intelligence and the heads of any other government entities involved in covert action

> To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters or other exceptionally sensitive matters . . . keep the intelligence committees fully and currently informed of all covert actions which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including significant failures.[18]

These are important provisions. At the higher levels of the political branches, program initiation receives more attention and consideration than program

administration. Moreover, policy-level oversight tends to focus on moments of crisis or failure and less on ensuring that programs are on track and in fact accomplishing what they were intended to achieve and in the manner contemplated and represented to the president.

Executive Process and Review

In addition to determining whether presidential approval is required, as a parallel matter, the definition of covert action also triggers specific processes of executive review. These processes are classified. However, in the wake of the Iran-*contra* scandal, President Reagan issued and released NSD-286, Approval and Review of Special Activities, describing the process the president intended apply to the review and authorization of covert activities. The document describes a process by which covert actions reviewed at working group level and then by the Deputies Committee and Principals Committee before submission to the president.[19] The public record also reflects that in establishing his National Security Council (NSC) system, President Clinton directed that "the Attorney General shall be invited to attend meetings pertaining to his jurisdiction, including covert actions."[20] Where the president has directed that a particular process of review occur, then he must authorize deviation from that process or otherwise delegate the authority to do so. Law or not, certainly the president should be informed when expected or important views are omitted from NSC consideration.

The special relationship between the president and the intelligence instrument is also recognized in executive directives as it is in statute. Executive Order 12333, for example, states: "The NSC shall act as the highest Executive Branch entity that provides review of, guidance for and direction to the conduct of all national foreign intelligence, counterintelligence, and special activities, and attendant policies and programs."[21]

This observation should not be lost on intelligence officials who disagree with policy or commentators who disagree with the acts of commission or omission placed at the CIA's door, rather than in the NSC Situation Room or the Oval Office.

Legal Permits and Constraints

In addition to authorizing covert activities, the law imposes certain constraints on the conduct of those activities. Of course, much of the relevant law is found in classified presidential and executive directives (e.g., attorney general guidelines and intelligence directives). "A finding may not authorize any action that would violate the Constitution or any statute of the United States."[22] This means that an otherwise lawful intelligence activity must comply with applicable U.S. law unless the law exempts the government or intelligence actors from its reach. This would include international law to the extent such law is incorporated

into U.S. law. For example, the law of armed conflict is found in the U.S. criminal code at Title 18, section 2441. Thus, when the United States placed the threat posed by Al Qaeda into a law of armed conflict construct before the embassy attacks in August 1998, this section of law became applicable to the conduct of covert activities against Osama bin Laden. This is evident in the instructions conveyed to certain Afghan "tribals," as reported by the 9/11 Commission. The instructions reference some of the staples of the law of armed conflict that one might expect to find on a military rules of engagement card, involving the treatment of prisoners and discrimination in attack. "The United States preferred that Bin Laden and his lieutenants be captured, but if a successful capture operation was not feasible, the tribals were permitted to kill them. The instructions added that the tribals must avoid killing others unnecessarily and must not kill or abuse Bin Ladin or his lieutenant if they surrendered."[23]

A prohibition on assassination, originally promulgated by President Ford in 1976, is documented in Executive Order 12333: "2.11 Prohibition on Assassination. No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination." This order continues in force, subject, like other executive orders, to classified presidential interpretation, amendment, or suspension. However, what is acknowledged publicly is that the targeting of legitimate military targets consistent with the law of armed conflict is not considered assassination under the executive order. As former National Security Advisor Samuel Berger testified before the 9/11 Commission with respect to the August 1998 (overt) missile strikes in Afghanistan: "We received rulings in the Department of Justice—[that the] executive order [did] not prohibit our ability—prohibit our effort to try to kill Bin Laden because it did not apply to situations in which you are acting in self-defense or you're acting against command and control targets against an enemy, which he certainly was."[24] As evidenced by parallel executive statements, similar conclusions were reached at the time of the 1986 U.S. air strikes on Tripoli, which included a tent used at times by Col. Muammar Qaddafi, and in April 2003 when the United States targeted buildings where Saddam Hussein was thought located.

In addition, "No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media."[25] For example, in the vernacular of intelligence law, the prospect of U.S. covert propaganda influencing the American media and public is known as blowback, a real risk in a global world with around-the-clock news cycles. As criminal lawyers will recognize, the critical term in the prohibition is *intended*, defining the restriction as one of specific intent. Of course, lawyers might find that the United States should be deemed to have intended something that is a predictable and logical consequence of action.

Regardless of legal argument, as a matter of legal policy, decision makers must evaluate the consequences of U.S. covert activities blowing back into the United States even where such a result is not intended. To pick a safe example, the

covert recruitment and insertion of a rebel force may lead unwitting policy observers to make unfounded conclusions about the strength of the opposition to a regime. Likewise, were the United States to covertly place favorable news articles in the foreign press, a historical mechanism for disseminating propaganda during the Cold War, the potential for blowback might hinge on whether the material was disseminated in English and/or in a forum likely to be covered by the U.S. media.

LEGAL PRISM

For the handful of lawyers who practice in this area, each covert activity will present questions of domestic, international, and foreign law. For example, in the context of a hypothetical extraordinary rendition, say, the kidnapping in 1960 of Nazi war criminal Adolf Eichmann by Israeli agents in Argentina, a lawyer might first determine whether the operation constitutes covert action, and if so whether it was authorized by an existing authority or required subsequent presidential approval. Whether considered covert or not, the operation must be approved in a manner consistent with internal U.S. directives, unclassified in the case of *The U.S. Attorney's Manual*, but otherwise generally classified. Depending on the circumstances, congressional notification might also be warranted or required.

U.S. criminal law and procedure might also be implicated depending on context. For example, if the subject was intended for U.S. prosecution, then lawyers would need to consider whether and how Fourth and Fifth Amendment protections might apply. Lawyers would also need to ensure that the means of abduction and transfer did not otherwise violate U.S. law, including the *Ker-Frisbie-Toscanino* doctrine—the concept that U.S. courts will generally not look to the manner by which a defendant came before the court so long as it did not involve conduct that "shocks the conscience."[26]

U.S., international, and foreign law relating to the Torture Convention might also be implicated.[27] In the case of foreign assistance or transfers, assurances involving the treatment of the subject might be required or prudent depending in part on the degree of U.S. involvement and direction during and after the rendition. Assurances may take different forms, including oral assurances, diplomatic notes, and liaison channel agreements. The government of the United Kingdom and the government of Jordan, for example, have concluded a public Memorandum of Understanding on the subject of rendition.[28] Whether assurances are required as a matter of law and in what form and level of authority will depend on context,[29] including for example, the track records of the country or persons involved, with respect to both their treatment of prisoners and adherence to prior assurances. Of course, the more intrusive the U.S. requirements, the less likely a third country or U.S. agents will agree to assist with a rendition.

International law might also be implicated with such an Eichmann rendition. Under international law, abduction without the meaningful consent of the host government would violate the territorial integrity of the host state and in all likelihood violate local law as well. However, as a matter of international law, the

violation of sovereignty would implicate the rights of the host state and not the subject of rendition. Call this the Eichmann Rule. In the Eichmann hypothetical, we will stipulate that the United States is not acting in self-defense or collective self-defense, but rather to vindicate the Nuremberg principles and the victims of the Holocaust. Such a rendition might also implicate bilateral treaties between the countries affected.

Such a rendition could also implicate the local (foreign) law of the jurisdiction where the rendition takes place and along the route of egress. Thus, even when an operation is conducted in a manner consistent with U.S. law, it may yet subject U.S. actors and others to criminal exposure in foreign states for kidnapping or for violating local law implementing international treaties or prescribing domestic rights. Such risks would need to be balanced against the importance of the seizure in question, the risk to bilateral relations (including the prospects for future extradition cooperation), as well as to multilateral efforts to bring war criminals to justice. Recall as well that in *Ker*, the Court did not object to the manner in which the defendant was brought before the court, but the Court suggested that Peru was not without recourse, for the extradition treaty between the United States and Peru "provides for the extradition of persons charged with kidnapping, and, on demand . . . the party who is guilty of it, *could* be surrendered" (emphasis added).[30]

LEGAL POLICY ISSUES

There are sometimes tensions between the requirements for successful action and the evaluation of the risks associated with covert action. On the one hand, successful covert action requires secrecy. In context, this is self-evident: if the intended policy effect will be lost if the U.S. hand is apparent; if the cost will outweigh the gain if the United States is held to account; or if the opportunity will be lost if the target is alerted. Secrecy is also generally essential to protect those persons engaged in the action. In context, covert action also requires speed. A terrorist target of opportunity may come and go in the wink of a Predator drone's eye. Moreover, covert activities occur within a context where the president has already determined that the action(s) in question "is important to the national security of the United States." These interests all point in the direction of a rapid, secret, and truncated process of authorization.

On the other hand, covert activities have historically carried significant policy risks. As a result, presidents have subjected covert activities to specialized processes of interagency and intra-agency review within the executive branch, and Congress has enacted a specialized process of notification. The Intelligence Committees have also adopted specialized internal procedures for addressing covert action, including a staff-directed quarterly review in the Senate. These parallel and sometime competing considerations result in a number of legal policy tensions.

What Is the Scope of the President's Authority over Covert Action in Wartime? What Role Must and Should Congress Play?

Heretofore the National Security Act has successfully served as an agreed mechanism between branches for addressing covert action. The act incorporates the ultimate constitutional positions of both branches (prior reporting and no reporting), without either side having conceded ultimate authority. The act leaves the political branches to work through the constitutional principles and tensions in an informal and contextual manner. In this way, the statute plays an overlooked but important constitutional role by defining expectations and suggesting limits—that is, setting the constitutional rules of the road between the president and Congress on the meaning and reporting requirements for covert action.

Thus, where the president and Congress have disagreed on an important point of law, they have also agreed to disagree and worked out accommodations. For example, when President Bush signed the 1990 Intelligence Authorization Act into law, he stated his constitutional view that he was not required to report findings in advance or at all; but in a side letter to the chairmen of the Intelligence Committees, Bush undertook as a matter of practice not to withhold notification to the Congress beyond a few days after signing a finding, understood on the Hill as within forty-eight hours.[31]

The question presented is whether these same constitutional rules of the road still abide, or should abide during wartime, and in particular during a conflict of indefinite duration. The question is all the more apt in light of presidential assertions of inherent authority to engage in certain electronic surveillance in wartime. The president (by which I mean a president, not necessarily the incumbent president) may assert a coterminous authority during "wartime" to engage in covert action outside the framework of the National Security Act or entirely within that provision of the National Security Act contemplating post facto notification. In the covert action context, there are arguments supporting a broad reading of presidential authority. Moreover, such a claim of authority would be impenetrable, provided the action in question in fact remained covert. However, the question is not just whether such a reading is lawful, but also whether it is a good idea.

APPRAISAL

Both the 9/11 Commission and the WMD Commission included recommendations to reform the manner in which Congress conducts intelligence oversight.[32] In particular, the commissions were critical of the episodic and reactive nature of oversight, as well as the disparate sources of congressional input into the design and funding of intelligence. Congressional oversight is selective. Few members of Congress outside the committees possess the background to address intelligence issues. Moreover, by definition, the intelligence committees operate with the inherently inductive knowledge that comes from periodic briefings rather than daily contact with operators and policy makers. Members see only part of the

picture, and then only that part of the picture contained in executive talking points that have survived layers of editing and are designed to fend off policy or partisan attack. Moreover, where members do follow intelligence closely, the interest tends to flow toward the "sexy" areas and not to areas like computer interoperability and funding audits, where appraisal may be needed most. Recall that approximately 85 percent of intelligence funding is directed to the Department of Defense.[33]

Nonetheless, congressional appraisal of the covert action instrument remains an essential source of balance on executive action, in part because in this area it may be the only source of balance. This is not a matter of constitutional idealism, although it pertains to the rule of law, but a matter of national security efficacy. In a system of shared powers and separate branches, Congress can provide a source of legitimacy and constitutional safeguard to intelligence activities that are conducted outside the reach of public knowledge and review. At times, the committee members and staff may be the only persons outside the NSC process and relevant intelligence agencies aware of an activity, and certainly the only persons without a direct policy stake in the success or funding of the activity. Therefore, whether their views are desired or not, they may be the only source of outside perspective at the advent of activity.

Sustained conflict will involve difficult policy trade-offs that will require sustained public support—that means support from a majority of the population, not just the president's political base or party. Chances are if the executive cannot sell a policy to a few members of Congress, the executive will not be able to convince the American public or the international community that a program or activity was prudent and/or lawful if it is disclosed.

The president alone has the authority to wield the covert action tool and the bureaucratic wherewithal to do so effectively. However, that is not to say the president should not strive to maximize his authority through the involvement and validation of Congress. Whatever can be said of the president's independent authority to act, when he acts with the express or implied authorization of Congress he acts at the zenith of his authority.[34] Therefore, those who believe in the necessity of executive action to preempt and respond to security threats should favor legal arguments that maximize presidential authority.

The inclusion of an independent check on executive action also reduces the potential for mistake. That is because the executive takes particular care in what it tells the Congress. War Powers Reports may be bland, for example, but they do necessitate an internal process before they are submitted that causes senior officials to check their assumptions and their arguments one more time before they send the report to the president and then Congress. In similar fashion, in notifying Congress of covert action, executive branch actors may well determine whether they have, in fact, covered all the angles and addressed or mitigated divergent views.

Finally, risk taking in the field increases where the government exercises shared authority. Certainly, this statement is hard to empirically demonstrate; the

concept is nonetheless real. As reflected in statements made to the 9/11 Commission, there is a cultural perception in the intelligence community that there is danger in acting too aggressively when the authority to do so is unclear or subject to political change. Where authority is embedded in a written finding provided to Congress, intelligence actors are on surer footing. There can be no legitimate debate as to what was or was not authorized, unless the finding is itself ambiguous, and therefore no excuse for not leaning forward in execution.

Nor does the inclusion of the legislative branch *necessarily* undermine the requirements for speed and secrecy. Although it is hard to prove a negative or demonstrate a general truth from a single point, it is noteworthy that one of the most significant intelligence secrets briefed to the Gang of Eight in the terrorism context—the U.S. effort to capture or kill Osama bin Laden in the late 1990s did not leak.

Is the Definition of Covert Action Still Viable?

Concerns for security, speed, and flexibility may also drive activities that heretofore received internal and external appraisal as covert action into legal pockets or rubrics subject to less preview and review. The same result may occur as a product of the good faith application of law to fact. For example, activities historically considered covert actions may become common in the context of a global conflict with Islamic Jihadists and thus come to constitute "traditional military, law enforcement, and diplomatic activities." These same activities may also properly fall within the construct of "liaison."

COVERT ACTION AND LIAISON

Liaison involves the formal and informal ties between allied or like-minded intelligence services. As an intelligence function, it lies somewhere between collection and covert action. Liaison incorporates all that the United States brings to the collection table as well as all that foreign liaison services bring. This is particularly important in the area of human intelligence and counterterrorism where foreign services may have greater access based on ethnicity, nationality, proximity, or security focus. Moreover, a global collection effort is too broad for any one service, however competent, to successfully cover all the gaps.

However, liaison also entails action. Most liaison entails the routine passage of information that one might expect between allies. Closer to the edge of the liaison envelope there is a thin line between liaison and covert action. This line is in sight where, for example, U.S. information may not just inform a liaison ally but predictably result in the ally taking action on the basis of the intelligence provided. The provision of satellite photographs, for example, or information pinpointing the location of a weapons lab, might be used to inform defensive planning or as the missing link in a decision to take military action. In other circumstances, where the United States is itself engaging in action, say, an extraordinary rendition with the participation of the host nation, the activity may fall outside the

construct of covert action, because the U.S. role is indeed apparent (at least to the assisting government).

Liaison can carry all the policy implications, benefits, and risks of a covert activity. (Our liaison counterparts would not be any good at intelligence if they were not getting something in return for their assistance other than goodwill.) This is noteworthy because U.S. liaison relationships extend beyond a predictable ring of democracies. Moreover, there is additional policy risk with liaison, because generally liaison activities receive less formal executive review than covert action. Most intelligence liaison is considered internal intelligence agency activity.[35] Returning to the hypothetical extraordinary rendition of Eichmann, one might imagine that an intra-agency review of the operation might identify a different set of policy pros, cons, and risks than an interagency review might.

The legal question, in context, is how much involvement is too much, such that the activities should be considered U.S. covert action? The legal policy question is this: Are such activities subject to an adequate measure of preview and review to confirm that (1) we are accomplishing all that we can accomplish, but (2) that we do so cognizant of the policy and legal risks involved and where appropriate that we mitigate, curtail, or eliminate those risks?

MILITARY ACTIVITIES AND COVERT ACTION

As noted, the definition of *covert action* is action rather than actor based. However, uniformed military operations have historically not been considered or treated as covert activities. Thus, even if the definition is action-based, the exception for traditional military activities may effectively remove clandestine military operations from its reach. This legal paradigm is reinforced by the military's long-standing cultural aversion to covert action. This antipathy may reflect a desire to avoid the additional internal and external oversight that accrues to covert action, as well as a desire to avoid the occasional tarnish that emerges from the retrospective glitter of certain covert activities. It may also emulate the traditional differences in military outlook and focus between Special Forces and regular units.

The military–covert action bifurcation is significant in light of the importance of special operations in a worldwide conflict against Islamic Jihadists. As with liaison, the critical question is not whether an activity is covert action but whether those activities that raise the sorts of policy and legal risks that covert activities do are subject to a process of rigorous policy and legal preview before they are undertaken. This is important not just as a matter of law but as a matter of national security success.

The Nature and Scope of Review

With respect to activities that are encompassed within the definition of covert action, two legal policy questions linger: How much executive process is appropriate before a finding or MON is signed or authorization for a specific

operation given? How much detail should be specified in these documents beyond that necessary to satisfy the statutory requirements?

PROCESS AND APPRAISAL

There are good arguments for and against process. In the view of some, *process* itself is a euphemism for *bureaucracy*, pejorative meaning intended.[36] Bureaucracy can delay (if not lose) operational opportunity. Bureaucracy increases the prospect of security breach. And bureaucracy usually brings layers of lawyers with it.

At the same time, national security is not subject to the same processes of internal, external, or public evaluation that may occur in other public policy areas. Where appraisal is structural, as in the case of agency inspectors general, the focus of analysis is on the identification of retrospective fault, rather than the ingredients of prospective success. To start, national security programs, and certainly compartmented intelligence programs, are secret. Limits on external appraisal also derive from certain functional and structural aspects of national security decision making and the presidency, especially during war. First, where national security is concerned, the policy pressure to succeed is at its greatest. As James Madison observed, "Safety from external danger is [indeed] the most powerful director of national conduct."[37] For presidents, this responsibility is real, immediate, and sincere. As a result, as Justice Jackson observed of executive deliberation, "The tendency is strong to emphasize transient results upon policies . . . and lose sight of enduring consequences upon the balanced power structure of our Republic."[38] Furthermore, for a presidency conditioned to crisis and command, which is to say the modern presidency, appraisal is a difficult decisional function to implement. There is also less opportunity for appraisal because where national security activities are subject to external review, they are subject to doctrines of judicial and political deference.

Process can be good or bad. Good process should be viewed as a source of policy strength in an area of historical risk, rather than an impediment to operational success. Good process alerts decision makers to the pros and cons of contemplated action, including the benefits and risks of accomplishing the task covertly rather than overtly. Process also helps ensure that secret policies are consistent with overt policies, and where they are not, whether there is good reason for any divergence. In an area where U.S. actions are intended to be kept secret, policy makers and those actors who may become aware of the underlying acts (if not their impetus) must also know of their existence to avoid blowback or inadvertent disclosure.

Clearly, streamlined executive decision has advantages in speed and secrecy. Speed comes in part from the absence of objection or dissent. But there are also benefits in the foreknowledge of objection and the improvements in policy or execution that dissent might influence. Because the conflict against Islamic fundamentalism is a conflict fought over values with words and not just territory

with weapons, careful review also allows policy makers to balance the relative benefits and costs represented by both the means and ends of action. We may in fact do harm to our physical security by losing cooperation or moral leverage when we employ arguments and methods that address our safety but are perceived as contradicting the values we otherwise espouse and that will help to undermine the jihadist terrorist movement. This tension is surely found in the area of extraordinary rendition, where there are sometime difficult trade-offs between preventing attacks and intelligence gathering, on one hand, and public diplomacy and human rights, on the other hand. When these decisions are taken solely within security agencies, the trade-offs will invariably balance in favor of action, just as company grade infantry officers will generally lean toward force protection when faced with questions of proportional balance between physical security and securing local support. Generally, executive review tends to be more inclusive, and therefore more rigorous, when a decision is subject to interagency review and senior policy review than when it is subject to single agency review.

Additional checks do not necessarily eliminate mistakes; they diminish the potential for error. In the context of intelligence operations using military means, such as the use of a Predator drone to attack the enemy, covert or not, the value of rigorous process is obvious. The military, for example, uses multiple tiered computer modeling to assess the potential for collateral damage. Targets are validated through a tested and recognized staff process. In short, rigorous but timely processes can demonstrate confidence in policy choice, legal arguments, and a willingness to account for effect.

When process proves bureaucratic, the answer is not to remove internal mechanisms of appraisal but to streamline them. For example, a legal question can go straight to the attorney general sitting in the Oval Office. As noted earlier, in the case of immediate need, the act provides for oral authorization where "immediate action by the United States is required," in which case a contemporaneous notation of the president's decision shall be made and a written finding produced within forty-eight hours.[39]

SPECIFICITY

Policy makers and lawyers must also consider the measure of detail to include in a finding or MON. There exists a tension between the generic authorizing instrument that provides the greatest flexibility and the too-specific instrument, which may need amendment with every change in the field. From the standpoint of legal policy, such documents should be crafted with sufficient specificity so that it is clear to the president what he is approving and the policy implications and risks of doing so, including the risks of taking no action. When flexibility may be required—for example, where the geographic foci of activity may shift—there should also be sufficient authority to adjust in the field or a viable process to garner prompt policy consideration, such as approval by the Principals or Deputies Committees or an appropriate subset of them.

Operators will almost always push for more flexibility, as those familiar with headquarters-field relationships will appreciate. A worldwide threat from Jihadists requires worldwide authority to respond and do so on short or immediate time frames. However, presidents should be careful they do not go too far and surrender authority over the actual substance of decision. For one cannot have effective appraisal and accountability if there is no discernible standard against which to measure result. Moreover, presidential decision is an essential source of democratic legitimacy for actions taken in secret with limited or no external input or review. At the same time, field operatives should press for sufficient detail so that the policy intent is clear and operatives are protected from second-guessing in the event of failure, and therefore will take greater risks in accomplishing the intended objectives. Moreover, clear direction also helps mitigate against the conscious and subconscious bias toward risk taking or risk aversion that individual case officers may possess.

CONCLUSION

Faced with an intractable opponent intent on catastrophic attack, the United States should respond with all the lawful national security tools. This includes covert action, which is fast, flexible, and often daring. It is also suited to a conflict that is as dependent on public diplomacy as it is on military action.

The success or failure of its use will depend on the successful assessment and allocation of risks. First, intelligence decision makers will have to find the optimum balance between counterintelligence risk and operational need. Effective penetration of terrorist targets requires the employment or utilization of persons with necessary ethnic and cultural background. These persons may not be U.S. citizens, and if they are, the ordinary degree of background inquiry may not be available. If we assume too little risk of counterintelligence penetration, we may forgo important opportunities. If we assume too much risk, we may find our agents and officers dead, our avenues of intelligence attack compromised, and our moral leadership undermined.

Second, the mission requires modulation of the risk the United States is prepared to assume in introducing U.S. personnel into high-risk environments, with the encompassing danger that Americans will be captured or killed. Intelligence operations on this battlefield are exceptionally dangerous where the opponent does not play by the "rules of the road" that state intelligence services generally accepted during the Cold War.

Intelligence policy makers will also have to factor in the risk of moral or legal compromise. Although lawful, is an operation a good idea? Do the potential benefits outweigh the policy costs? Have decision makers identified and weighed the enduring consequences of their actions or just their immediate results? If one, for instance, works back from the threat of a WMD being used in a major U.S.

city or that of an ally, then one must hope that the government is continuously appraising and reappraising how we have balanced these risks.

Covert action law addresses these risks in two main ways. First, in statute and executive directive, the law imposes certain minimum requirements of process to address the policy and legal risks and trade-offs of action. Second, the law establishes clarity in accountability. In some cases this is done through imposition of substantive limits on conduct. But more directly, the law does so by making it clear that the president is responsible. Where covert action is concerned, the buck does indeed stop on the president's desk.

However, law does not dictate results; it provides opportunity for success. Changes in the legal landscape will occur because the definition of covert action is, by its own terms, evolving. Moreover, as the United States moves from Cold War understandings to Long War applications of the intelligence and military instruments, a broad range of activities important to national security will be conducted as liaison or clandestine military operations. As a result, the success or failure of covert operations will not only depend on how the executive uses the covert action instrument but on the measure of process applied to those activities that bear comparable benefits and risks.

NOTES

1. Covert action is one of the five intelligence functions along with collection, analysis and dissemination, liaison, and counterintelligence. R. Gates, "The CIA and Foreign Policy," *Foreign Affairs* 66, no. 2 (Winter 1987/88), p. 216.

2. For a historical overview see, G. Treverton, *Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, 1987); M. Reisman and J. Baker, *Regulating Covert Action* (New Haven, CT: Yale University Press, 1992).

3. See Central Intelligence Agency (undated), *Intelligence in the War of Independence*, available at http://www.cia.gov/cia/publications/warindep/index.html (accessed March 10, 2006); for additional historic perspective, see S. Knott, "Thomas Jefferson's Clandestine Foreign Policy," *International Journal of Intelligence and Counterintelligence* 4, no. 3 (Fall 1990).

4. The words of the Doolittle Committee capture the tenure: "It is now clear that we are facing an implacable enemy whose avowed objective is world domination by whatever means ate whatever cost. There are no rules in such a game. Hitherto acceptable norms of human conduct do not apply." "Report on the Covert Activities of the Central Intelligence Agency," September 30, 1954.

5. See, for example, *Totten Administrator v. United States*, 92 U.S. 105 (1875) and its 2005 antecedent *Tenet et al. v. Doe et ux, 544* U.S. __ (2005); *Curtiss-Wright Export Corp. v. United States*, 299 U.S. 304 (1936); *United States v. Nixon*, 418 U.S. 683 (1974). See also, Reisman and Baker, *Regulating Covert Action*, pp. 117–18.

6. In addition to the president's constitutional authority, covert action was undertaken pursuant to §102(d)(5) of the National Security Act: "It shall be the duty of the Agency, under the direction of the National Security Council . . . (5) to perform such other

functions and duties relating to intelligence affecting the national security as the National Security Council may from time to time direct." Reisman and Baker, *Regulating Covert Action*, p. 118.

7. 50 U.S.C. § 413b(e) (2006).

8. 50 U.S.C. §§ 413b(e)(1), (2), (3), and (4) (2006).

9. Senate Report No. 102-85, "Legislative History, Intelligence Authorization Act of 1990," P.L. 102-88, p. 235.

10. For a discussion of the etymology of the phrase "national security" see M. Shulman, "The Progressive Era Origins of the National Security Act," *Dickinson. Law Review* 104 (Winter 2000), p. 289.

11. 50 U.S.C. § 413b(a) (2006).

12. 50 U.S.C. § 413b(c)(1) (2006).

13. 50 U.S.C. § 413b(c)(2) (2006).

14. 50 U.S.C. § 413b(c)(3) (2006).

15. Senate Report No. 102-85, p. 234.

16. Ronald Reagan, National Security Decision Directive 286, "Approval and Review of Special Activities," October 15, 1987.

17. 50 U.S.C. § 413(a)(1) (2006).

18. 50 U.S.C. § 413(a) (2006), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458 §1071(a)(Y).

19. The NSC is comprised of the president, vice president, secretary of State, and secretary of Defense. The director of National Intelligence and the chairman of the Joint Chiefs of Staff are statutory advisors to the NSC. The president designates members of the NSC Principals Committee and the NSC Deputies Committee. Membership may vary depending on the subject matter. In general, the Principals Committee is chaired by the assistant to the president for National Security Affairs and is comprised of the secretary of State, secretary of Defense, the DNI, the chairman of the Joint Chiefs, the national security advisor to the vice president, and, depending on the subject matter, the attorney general, and the secretary of the Treasury. Depending on the president, the chief of staff to the president, the secretary of the Treasury, the U.S. Ambassador to the United Nations, and others have been designated members of the Principals Committee. The Deputies Committee generally is chaired by the principal deputy assistant to the president for National Security Affairs and is comprised of the deputies or designated representatives of the Principals. Of course, other senior officials and staff may attend designated meetings of the committees.

20. William J. Clinton, Presidential Decision Directive (PDD) 2, "Organization of the National Security Council," January 20, 1993, para. A.

21. Executive Order 12333, "Intelligence Activities," December 4, 1981, para. 1.2(a). Special activities are "activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly . . . ," in other words "covert action."

22. 50 U.S.C. § 513b(a)(5) (2006).

23. The 9/11 Commission, *Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: Norton, 2004), p. 132. See also R. Posner, "The 9/11 Report: A Dissent," *New York Times Book Review*, August 29, 2004.

24. September 18, 2002 Testimony before Senate and House Select Committees on Intelligence.

25. 50 U.S.C. § 413b(f) (2006).

26. See generally, *Ker v. Illinois*, 119 U.S. 436 (1886); *Frisbie v. Collins*, 342 U.S. 519 (1952); *Toscanino v. United States*, 500 F.2d 267 (2nd Cir. 1974); and *United States v. Alvarez-Machain*, 504 U.S. 655 (1992). The doctrine is discussed in Reisman and Baker, *Regulating Covert Action*, pp. 128–30.

27. Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, and 18 U.S.C. § 2340A.

28. "Memorandum of Understanding Between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the Hashemite Kingdom of Jordan Regulating the Provision of Undertakings in Respect of Specified Persons Prior to Deportation," August 10, 2005, available at http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/uk/4143214.stm (accessed March 10, 2006).

29. In the context of detainees transferred from Guantánamo Bay to third countries, the assistant U.S. attorney representing the United States in litigation has stated in court: "We have obtained assurances before they are released that it is more likely than not that they will not be tortured in a country that they go to. In fact it has happened where we have not been satisfied with the assurances that a foreign government has given the United States, and we have not transferred those detainees." V. Blum, "Gaining a Foothold in Guantanamo: Defense Lawyers Want Access to Every Detainee—And Say in Prisoner Transfers," *Legal Times*, March 28, 2005.

30. *Ker*, 444.

31. Senate Report 102-85, p. 233, quoting the text of a letter sent to the chairmen of the Senate and House Intelligence Committees. "Dear Mr. Chairman: I am aware of your concerns regarding the provision of notice Congress of covert action. . . . I anticipate that in almost all instances, prior notice will be possible. In those rare instances where prior notice is not provided, I anticipate that notice will be provided within a few days. Any withholding beyond this period will be based upon my assertion of authorities granted to this office by the Constitution." For an example of an instance when a president might withhold notification occurring before these provisions were enacted see S. Turner, "Covert Common Sense: Don't Throw the CIA out with the Ayatollah," *Washington Post,* November 23, 1986.

32. See 9/11 Commission, *Final Report*, pp. 419–23; Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington: Government Printing Office, 2005), pp. 337–41.

33. Congressional Research Service, "Director of National Intelligence: Statutory Authorities," April 11, 2005, p. 2; Commission on the Roles and Capabilities of the Intelligence Community, p. 45, available at http://www.access.gpo.gov/intelligence/int/pdf/report.html (accessed March 14, 2006).

34. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635–36 (1952).

35. Like covert action, liaison authority is expressly authorized in statute and unclassified executive directive. Section 104(e), for example, of the National Security Act includes within the DNI's authorities "Coordination with Foreign Governments." Specifically, "under the direction of the National Security Council . . . the Director shall coordinate the relationships between elements of the intelligence community and the intelligence security services of foreign governments on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine

means." Liaison might also be conducted solely pursuant to the president's constitutional authority as delegated by directive. Executive Order 12333 directs the (then) DCI to "Formulate policies concerning foreign intelligence and counterintelligence arrangements with foreign governments, coordinate foreign intelligence and counterintelligence relationships between agencies of the Intelligence community and the intelligence and or internal security services of foreign governments, and establish procedures governing the conduct of liaison by any department or agency with such services on narcotics matters."

36. J. Lehman. "Getting Spy Reform Wrong; Sept. 11 Commission's Proposals Were Turned into Bureaucratic Bloat," *Washington Post*, November 16, 2005.

37. A. Hamilton, J. Madison, and J. Jay, *The Federalist Papers,* edited by Clinton Rossiter (New York: Signet, 1961), p. 67.

38. *Youngstown*, 343 U.S. at 634.

39. 500 U.S.C. 413b (a) (2006).

APPENDIX A

EXCERPT FROM THE CHURCH COMMITTEE REPORT ON THE EVOLUTION OF CIA COVERT ACTION

CLANDESTINE ACTIVITIES

A. ORIGINS OF COVERT ACTION

The concept of a central intelligence agency developed out of a concern for the quality of intelligence analysis available to policymakers. The 1945 discussion which surrounded the creation of CIG focused on the problem of intelligence coordination. Two years later debates on the CIA in the Congress and the Executive assumed only the coordination role along with intelligence collection (both overt and clandestine) and analysis for the newly constituted Agency.

Yet, within one year of the passage of the National Security Act, the CIA was charged with the conduct of covert psychological, political, paramilitary, and economic activities.[21] The acquisition of this mission had a profound impact on the direction of the Agency and on its relative stature within the government.

The precedent for covert activities existed in OSS. The clandestine collection capability had been preserved through the Strategic Services Unit, whose responsibilities CIG absorbed in June 1946. The maintenance of that capability and its presence in CIA contributed to the Agency's ultimate assumption of a covert operational role.

Source: Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee), *Supplementary Detailed Staff Reports on Foreign And Military Intelligence, Final Report,* Book IV, 94th Cong., 2d Sess., Sen. Rept. No. 94–755 (April 23, 1976), pp. 25–41 (written by staff member Dr. Anne Karalekas). Footnotes reflect original numbering.

[21] Psychological operations were primarily media-related activities, including unattributed publications, forgeries, and subsidization of publications; political action involved exploitation of dispossessed persons and defectors, and support to political parties; paramilitary activities included support to guerrillas and sabotage; economic activities consisted of monetary operations.

The United States, initiation of covert operations is usually associated with the 1948 Western European elections. It is true that this was the first officially recorded evidence of U.S. covert political intervention abroad. However, American policymakers had formulated plans for covert action—at first covert psychological action—much earlier. Decisions regarding U.S. sponsorship of clandestine activities were gradual but consistent, spurred on by the growing concern over Soviet intentions.

By late 1946, cabinet officials were preoccupied with the Soviet threat, and over the next year their fears intensified. For U.S. policymakers, international events seemed to be a sequence of Soviet incursions. In March 1946, the Soviet Union refused to withdraw its troops from the Iranian province of Azerbaijan; two months later civil war involving Communist rebel forces erupted in Greece. By 1947, Communists had assumed power in Poland, Hungary, and Rumania; and in the Phillipines the government was under attack by the Hukbalahaps, a communist-led guerrilla group.

For U.S. officials, the perception of the Soviet Union as a global threat demanded new modes of conduct in foreign policy to supplement the traditional alternatives of diplomacy and war. Massive economic aid represented one new method of achieving U.S. foreign policy objectives. In 1947, the United States embarked on an unprecedented economic assistance program to Europe with the Truman Doctrine and the Marshall Plan. By insuring economic stability, U.S. officials hoped to limit Soviet encroachments. Covert operations represented another, more activist departure in the conduct of U.S. peacetime foreign policy. Covert action was an option that was something more than diplomacy but still short of war. As such, it held the promise of frustrating Soviet ambitions without provoking open conflict.

The suggestion for the initiation of covert operations did not originate in CIG. Sometime in late 1946, Secretary of War Robert Patterson suggested to Forrestal that military and civilian personnel study this form of war for future use. What prompted Patterson's suggestion is unclear. However, from Patterson's suggestion policymakers proceeded to consider the lines of authority for the conduct of psychological operations. Discussion took place in the State-War-Navy Coordinating Committee (SWNCC), whose members included the Secretaries of the three Departments, Byrnes, Patterson and Forrestal.[22] In December 1946, a SWNCC subcommittee formulated guidelines for the conduct of psychological warfare in peacetime and wartime.[23] The full SWNCC adopted the recommendation later that month.

Discussion continued within the Executive in the spring and summer of 1947. From all indications, only senior-level officials were involved, and the discussions were closely held. From establishing guidelines for the possibility of psychological warfare, policymakers proceeded to contingency planning. On April 30, 1947, a SWNCC subcommittee was organized to consider and actually plan for a U.S. psychological warfare effort. On June 5, 1947, the subcommittee was accorded a degree of permanency and renamed the

[22] SWNCC was established late in 1944 as an initial attempt at more centralized decisionmaking.

[23] In peacetime, psychological warfare would be directed by an interdepartmental subcommittee of SWNCC with the approval of the JCS and the National Intelligence Authority. During war, a Director of Psychological Warfare would assume primary responsibility under a central committee responsible to the President. The committee would consist of representatives from the SWNCC and from CIG.

Special Studies and Evaluations Subcommittee. By this time, the fact that the U.S. would engage in covert operations was a given; what remained were decisions about the organizational arrangements and actual implementation. Senior officials had moved from the point of conceptualization to determination of a specific need. Yet it is not clear whether or not they had in mind specific activities geared to specific countries or events.

In the fall of 1947 policymakers engaged in a series of discussions on the assignment of responsibility for the conduct of covert operations. There was no ready consensus and a variety of opinions emerged. DCI Hillenkoetter had his own views on the subject. Sometime in October 1947 he recommended "vitally needed psychological operations"—again in general terms without reference to specific countries or groups—but believed that such activities were military rather than intelligence functions and therefore belonged in an organization responsible to the JCS. Hillenkoetter also believed congressional authorization would be necessary both for the initiation of psychological warfare and for the expenditure of funds for that purpose. Whatever Hillenkoetter's views on the appropriate authorization for a psychological warfare function, his opinions were undoubtedly influenced by the difficulties he had experienced in dealing with the Departments. It is likely that he feared CIA's acquisition of an operational capability would precipitate similar problems of departmental claims on the Agency's operational functions. Hillenkoetter's stated preferences had no apparent impact on the outcome of the psychological warfare debate.

Within a few weeks of Hillenkoetter's statement, Forrestal, the Secretaries of the Army, Navy, and Air Force, along with the JCS, advanced their recommendations regarding the appropriate organization to conduct covert psychological warfare. In a proposal dated November 4, they held that propaganda of all kinds was a function of the State Department and that an Assistant Secretary of State in consultation with the DCI and a military representative should be responsible for the operations.

On November 24, President Truman approved the November 4 recommendation, assigning psychological warfare coordination to the Secretary of State. Within three weeks, the decision was reversed. Despite the weight of numbers favoring State Department control, the objections of Secretary of State George Marshall eliminated the option advanced by the other Secretaries. Marshall opposed State Department responsibility for covert action. He was vehement on the point and believed that such activities, if exposed as State Department actions, would embarrass the Department and discredit American foreign policy both short-term and long-term.

Apart from his position as Secretary of State, the impact of Marshall's argument derived from the more general influence he exerted at the time. Marshall had emerged from the war as one of America's "silent heroes." To the public, he was a quiet, taciturn, almost unimpressive figure, but as the Army Chief of Staff during the war, he had gained the universal respect of his civilian and military colleagues for his commitment, personal integrity, and ability.

In the transition from military officer to diplomat, he had developed a strong sense that the United States would have to adopt an activist role against the Soviet Union. Immediately after his appointment as Secretary in February 1947, he played a key role in the decision to aid Greece and Turkey and quickly after, in June 1947, announced the sweeping European economic recovery program which bore his name. It was out of concern for the success and credibility of the United States' recently articulated economic program that Marshall objected to State Department conduct of covert action. Marshall favored placing covert activities outside the Department, but still subject to guidance from the Secretary of State.

Marshall's objections prevailed, and on December 14 the National Security Council adopted NSC 4/A, a directive which gave the CIA responsibility for covert psychological operations. The DCI was charged with ensuring that psychological operations were consistent with U.S. foreign policy and overt foreign information activities. On December 22 the Special Procedures Group was established within the CIA's Office of Special Operations to carry out psychological operations.

Although Marshall's position prevented State from conducting psychological warfare, it does not explain why the CIA was charged with the responsibility. The debate which ensued in 1947 after the agreement on the need for psychological warfare had focused on control and responsibility. At issue were the questions of who would plan, direct, and oversee the actual operations.

State and the military wanted to maintain control over covert psychological operations, but they did not want to assume operational responsibility. The sensitive nature of the operations made the Departments fear exposure of their association with the activities. The CIA offered advantages as the organization to execute covert operations. Indeed, in 1947 one-third of the CIA's personnel had served with OSS. The presence of former OSS personnel, who had experience in wartime operations, provided the Agency with a group of individuals who could quickly develop and implement programs. This, coupled with its overseas logistical apparatus, gave the Agency a ready capability. In addition, the Agency also possessed a system of unvouchered funds for its clandestine collection mission, which meant that there was no need to approach Congress for separate appropriations. With the Departments unwilling to assume the risks involved in covert activities, the CIA provided a convenient mechanism.

During the next six months psychological operations were initiated in Central and Eastern Europe. The activities were both limited and amateur and consisted of unattributed publications, radio broadcasts, and blackmail. By 1948 the Special Procedures Group had acquired a radio transmitter for broadcasting behind the Iron Curtain, had established a secret propaganda printing plant in Germany, and had begun assembling a fleet of balloons to drop propaganda materials into Eastern European countries.

Both internally and externally the pressure continued for an expansion in the scope of U.S. covert activity. The initial definition of covert action had been limited to covert psychological warfare. In May 1948, George F. Kennan, Director of the State Department's Policy Planning Staff, advocated the development of a covert political action capability. The distinction at that time was an important and real one. Political action meant direct intervention in the electoral processes of foreign governments rather than attempts to influence public opinion through media activities.

International events gave force to Kennan's proposal. In February 1948, Communists staged a successful coup in Czechoslovakia. At the same time, France and Italy were beleaguered by a wave of Communist-inspired strikes. In March 1948, near hysteria gripped the U.S. Government with the so-called "war scare." The crisis was precipitated by a cable from General Lucius Clay, Commander in Chief, European Command, to Lt. General Stephen J. Chamberlin, Director of Intelligence, Army General Staff, in which Clay said, "I have felt a subtle change in Soviet attitude which I cannot define but which now gives me a feeling that it [war] may come with dramatic suddenness."

The war scare launched a series of interdepartmental intelligence estimates on the likelihood of a Soviet attack on Western Europe and the United States. Although the estimates concluded that there was no evidence that the U.S.S.R. would start a war, Clay's

cable had articulated the degree of suspicion and outright fear of the Soviet Union that was shared by policymakers at this time. Kennan proposed that State, specifically the Policy Planning Staff, have a "directorate" for overt and covert political warfare. The director of the Special Studies Group, as Kennan named it, would be under State Department control, but not formally associated with the Department. Instead, he would have concealed funds and personnel elsewhere, and his small staff of eight people would be comprised of representatives from State and Defense.

Kennan's concept and statement of function were endorsed by the NSC. In June 1948, one month after his proposal, the NSC adopted NSC 10/2, a directive authorizing a dramatic increase in the range of covert operations directed against the Soviet Union, including political warfare, economic warfare, and paramilitary activities.

While authorizing a sweeping expansion in covert activities, NSC 10/2 established the Office of Special Projects, soon renamed the Office of Policy Coordination (OPC), within the CIA to replace the Special Procedures Group. As a CIA component OPC was an anomaly. OPC's budget and personnel were appropriated within CIA allocations, but the DCI had little authority in determining OPC's activities. Responsibility for the direction of OPC rested with the Office's director, designated by the Secretary of State. Policy guidance—decisions on the need for specific activities—came to the OPC director from State and Defense, bypassing the DCI.

The organizational arrangements established in 1948 for the conduct of covert operations reflected both the concept of covert action as defined by U.S. officials and the perception of the CIA as an institution. Both the activities and the institution were regarded as extensions of State and the military services. The Departments (essentially the NSC) defined U.S. policy objectives; covert action represented one means of attaining those objectives; and the CIA executed the operations.

In a conversation on August 12, 1948, Hillenkoetter, Kennan, and Sidney Souers discussed the implementation of NSC 10/A. The summary of the conversation reveals policymakers firm expectation that covert political action would serve strictly as a support function for U.S. foreign and military policy and that State and the services would define the scope of covert activities in specific terms. The summaries of the participants' statements as cited in a CIA history bear quoting at length:

> Mr. Kennan made the point that as the State Department's designated representative he would want to have specific knowledge of the objectives of every operation and also of the procedures and methods employed in all cases where those procedures and methods involved political decisions.
>
> Mr. Souers indicated his agreement with Mr. Kennan's thesis and stated specifically that it has been the intention of the National Security Council in preparing the document that it should reflect the recognition of the principle that the Departments of State and the National Military Establishment are responsible for the conduct of the activities of the Office of Special Projects, with the Department of State taking preeminence in time of peace and the National Military Establishment succeeding the pre-eminent position in wartime.
>
> Admiral Hillenkoetter agreed with Mr. Kennan's statement that the political warfare activity should be conducted as an instrument of U.S. foreign policy and subject in peacetime to direct guidance by the State Department.
>
> Mr. Kennan agreed that it was necessary that the State Department assume responsibility for stating whether or not individual projects are politically desirable and stated that as the State Department's designated representative he would be accountable for providing such decisions.

Likewise, reflecting on his intentions and those of his colleagues in 1948, Kennan recently stated:

> . . . we were alarmed at the inroads of the Russian influence in Western Europe beyond the point where the Russian troops had reached. And we were alarmed particularly over the situation in France and Italy. We felt that the Communists were using the very extensive funds that they then had in hand to gain control of key elements of life in France and Italy, particularly the publishing companies, the press, the labor unions, student organizations, women's organizations, and all sort of organizations of that sort, to gain control of them and use them as front organizations. . . .
>
> That was just one example that I recall of why we thought that we ought to have some facility for covert operations. . . .
>
> . . . It ended up with the establishment within CIA of a branch, an office for activities of this nature, and one which employed a great many people. It did not work out at all the way I had conceived it or others of my associates in the Department of State. We had thought that this would be a facility which could be used when and if an occasion arose when it might be needed. There might be years when we wouldn't have to do anything like this. But if the occasion arose we wanted somebody in the Government who would have the funds, the experience, the expertise to do these things and to do them in a proper way.[24]

Clearly, in recommending the development of a covert action capability in 1948, policymakers intended to make available a small contingency force that could mount operations on a limited basis. Senior officials did not plan to develop large-scale continuing covert operations. Instead, they hoped to establish a small capability that could be activated at their discretion.

B. THE OFFICE OF POLICY COORDINATION, 1948–1952

OPC developed into a far different organization from that envisioned by Forrestal, Marshall, and Kennan in August 1948. By 1952, when it merged with the Agency's clandestine collection component, the Office of Special Operations, OPC had expanded its activities to include worldwide covert operations, and it had achieved an institutional independence that was unimaginable at the time of its inception.

The outbreak of the Korean War in the summer of 1950 had a significant effect on OPC. Following the North Korean invasion of South Korea, the State Department as well as the Joint Chiefs of Staff recommended the initiation of paramilitary activities in Korea and China. OPC's participation in the war effort contributed to its transformation from an organization that was to provide the capability for a limited number of *ad hoc* operations to an organization that conducted continuing, ongoing activities on a massive scale. In concept, manpower, budget, and scope of activities, OPC simply skyrocketed. The comparative figures for 1949 and 1952 are staggering. In 1949 OPC's total personnel strength was 302; in 1952 it was 2,812 plus 3,142 overseas contract personnel. In 1949 OPC's budget figure was $4,700,000; in 1952 it was $82,000,000. In 1949, OPC had personnel assigned to seven overseas stations; in 1952 OPC had personnel at forty-seven stations.

Apart from the impetus provided by the Korean War several other factors converged to alter the nature and scale of OPC's activities. First, policy direction took the form of condoning and fostering activity without providing scrutiny and control. Officials

[24] George F. Kennan testimony, October 28 1975, pp. 8–10.

throughout the government regarded the Soviet Union as an aggressive force, and OPC's activities were initiated and justified on the basis of this shared perception. The series of NSC directives which authorized covert operations laid out broad objectives and stated in bold terms the necessity for meeting the Soviet challenge head on. After the first 1948 directive authorizing covert action, subsequent directives in 1950 and 1951 called for an intensification of these activities without establishing firm guidelines for approval.

On April 14, 1950, the National Security Council issued NSC 68, which called for a non-military counter-offensive against the U.S.S.R., including covert economic, political, and psychological warfare to stir up unrest and revolt in the satellite countries. A memo written in November 1951 commented on the fact that such broad and comprehensive undertakings as delineated by the NSC could only be accomplished by the establishment of a worldwide structure for covert operations on a much grander scale than OPC had previously contemplated. The memo stated:

> It would be a task similar in concept, magnitude and complexity to the creation of widely deployed military forces together with the logistical support required to conduct manifold, complex and delicate operations in a wide variety of overseas locations.

On October 21, 1951 NSC 10/5 replaced NSC 10/2 as the governing directive for covert action. It once again called for an intensification of covert action and reaffirmed the responsibility of the DCI in the conduct of covert operations. Each of these policy directives provided the broadest justification for large-scale covert activity.

Second, OPC operations had to meet the very different policy needs of the State and Defense Departments. The State Department encouraged political action and propaganda activities to support its diplomatic objectives, while the Defense Department requested paramilitary activities to support the Korean War effort and to counter communist-associated guerrillas. These distinct missions required OPC to develop and maintain different capabilities, including manpower and support material.

The third factor contributing to OPC's expansion was the organizational arrangements that created an internal demand for projects. The decision to undertake covert political action and to lodge that responsibility in a group distinct from the Departments required the creation of a permanent structure. OPC required regular funding to train and pay personnel, to maintain overseas stations (and provide for the supporting apparatus), and to carry out specific projects. That funding could not be provided on an *ad hoc* basis. It had to be budgeted for in advance. With budgeting came the need for ongoing activities to justify future allocations—rather than leaving the flexibility of responding to specific requirements.

To fulfill the different State and Defense requirements OPC adopted a "project" system rather than a programmed financial system. This meant that operations were organized around projects—individual activities, e.g. funding to a political candidate—rather than general programs or policy objectives, and that OPC budgeted in terms of anticipated numbers of projects. The project system had important internal effects. An individual within OPC judged his own performance, and was judged by others, on the importance and number of projects he initiated and managed. The result was competition among individuals and among the OPC divisions to generate the maximum number of projects. Projects remained the fundamental units around which clandestine activities were organized, and two generations of Agency personnel have been conditioned by this system.

The interaction among the OPC components reflected the internal competition that the project system generated. OPC was divided between field personnel stationed overseas and Headquarters personnel stationed in Washington. Split into four functional staffs (dealing with political warfare, psychological warfare, paramilitary operations and economic warfare) and six geographical divisions, Headquarters was to retain close control over the initiation and implementation of projects to insure close policy coordination with State and Defense. Field stations were to serve only as standing mechanisms for the performance of tasks assigned from Washington.

The specific relationship between the functional staffs, the geographical divisions and the overseas stations was intended to be as follows: With guidance from the NSC, the staffs would generate project outlines for the divisions. In turn, the divisions would provide their respective overseas stations with detailed instructions on project action. Very soon, however, each of the three components was attempting to control project activities. Within the functional staffs proprietary attitudes developed toward particular projects at the point when the regional divisions were to take them over. The staffs were reluctant to adopt an administrative support role with respect to the divisions in the way that was intended. Thus, the staffs and the divisions began to look upon each other as competitors rather than joint participants. In November 1949 an internal study of OPC concluded that:

> . . . the present organization makes for duplication of effort and an extensive amount of unnecessary coordination and competition rather than cooperation and teamwork. . . .

A reorganization in 1950 attempted to rectify the problem by assigning responsibility for planning single-country operations to the appropriate geographical division. This meant that the divisions assumed real operational control. The staffs were responsible for coordinating multiple country operations as well as providing the guidance function. In principle the staffs were to be relegated to the support role they were intended to serve. However, the break was never complete. The distinctions themselves were artificial, and staffs seized on their authority over multiple country activities to maintain an operational role in such areas as labor operations. This tension between the staffs and the divisions continued through the late 1960's as some staffs achieved maximum operational independence. The situation is a commentary on the project orientation which originated with OPC and the recognition that promotion and rewards were derived from project management—not from disembodied guidance activities.

The relationship between Washington and the field was subject to pressures similar to those that influenced the interaction between the divisions and the staffs. Predictably, field personnel began to develop their own perspective on suitable operations and their mode of conduct. Being "there," field personnel could and did argue that theirs was the most realistic and accurate view. Gradually, as the number of overseas personnel grew and as the number of stations increased, the stations assumed the initiative in project development.

The regional divisions at Headquarters tended to assume an administrative support role but still retained approval authority for projects of particular sensitivity and cost. The shift in initiative first from the staffs to the divisions, then to the stations, affected the relative desirability of assignments. Since fulfillment of the OPC mission was measured in terms of project development and management, the sought-after places were those where the projects originated. Individuals who were assigned those places rose quickly within the Directorate.

C. POLICY GUIDANCE

Responsibility for coordination with the State and Defense Departments rested with Frank G. Wisner, appointed Assistant Director for Policy Coordination (ADPC) on September 1, 1948. Described almost unanimously by those who worked with him as "brilliant," Wisner possessed the operational instincts, the activist temperament, and the sheer physical energy required to develop and establish OPC as an organization. Wisner also had the advantages of independent wealth and professional and social contacts which he employed skillfully in advancing OPC's position within the Washington bureaucracy.

Wisner was born into a prominent Southern family and distinguished himself as an undergraduate and a law student at the University of Virginia. Following law school, Wisner joined a New York law firm where he stayed for seven years. After a brief stint in the Navy, Wisner was assigned to OSS and spent part of his time serving under Allen Dulles in Wiesbaden, Germany. At the end of the war he returned to law practice, but left again in 1947 to accept the post of Deputy to the Assistant Secretary of State for Occupied Areas. It was from this position that Wisner was tapped to be ADPC.

Although the stipulation of NSC 10/2 that the Secretary of State designate the ADPC was intended to insure the ADPC's primary identification with State, that did not occur. Wisner quickly developed an institutional loyalty to OPC and its mission and drew on the web of New York law firm connections that existed in postwar Washington as well as on his State Department ties to gain support for OPC's activities.

The guidance that State and Defense provided OPC became very general and allowed the maximum opportunity for project development. Approximately once a week Wisner met with the designated representatives of State and Defense. Given that Kennan had been a prime mover in the establishment of OPC, it was unlikely that as the State Department's designated representative from 1948 to 1950 he would discourage the overall direction of the organization he had helped create. From 1948 to 1949 Defense was represented by General Joseph T. McNarney, the former Commander of U.S. Forces in Europe. Having stood "eyeball to eyeball" with the Russians in Germany, McNarney was highly sympathetic to the OPC mission.

With the broad objectives laid out in NSC 10/2, the means of implementation were left to OPC. The representatives were not an approval body, and there was no formal mechanism whereby individual projects had to be brought before them for discussion. Because it was assumed that covert action would be exceptional, strict provisions for specific project authorization were not considered necessary. With minimal supervision from State and Defense and with a shared agreement on the nature of the OPC mission, individuals in OPC could take the initiative in conceiving and implementing projects. In this context, operational tasks, personnel, money and material tended to grow in relation to one another with little outside oversight.

In 1951, DCI Walter Bedell Smith took the initiative in requesting more specific high-level policy direction. In May of that year, after a review of NSC 68, Smith sought a clarification of the OPC mission from the NSC.[26] In a paper dated May 8, 1951, entitled the "Scope and Pace of Covert Operations" Smith called for NSC restatement or

[26] Soon after his appointment as DCI in October 1950, Smith succeeded in having OPC placed directly under the jurisdiction of the DCI, making Wisner responsible to him rather than to the Department of State and Defense. See pp. 37–38.

redetermination of the several responsibilities and authorities involved in U.S. covert operations. More importantly, Smith proposed that the newly created Psychological Strategy Board provide CIA guidance on the conduct of covert operations.[27]

The NSC adopted Smith's proposal making the Psychological Strategy Board the approval body for covert action. The body that had been responsible for exercising guidance over the CIA had received it from the DCI. Whatever the dimensions of the growth in OPC operations, the NSC had not attempted to limit the expansion.

D. OPC ACTIVITIES

At the outset OPC activities were directed toward four principal operational areas: refugee programs, labor activities, media development, and political action. Geographically, the area of concentration was Western Europe. There were two reasons for this. First, Western Europe was the area deemed most vulnerable to Communist encroachment; and second, until 1950 both CIA (OSO) and OPC were excluded from the Far East by General Douglas MacArthur, who refused to concede any jurisdiction to the civilian intelligence agency in the Pacific theater—just as he had done with OSS during the war.

OPC inherited programs from both the Special Procedures Group (SPG) and the Economic Cooperation Administration (ECA). After the issuance of NSC 10/2 SPG turned over to OPC all of its resources, including an unexpended budget of over $2 million, a small staff, and its communications equipment. In addition to SPG's propaganda activities OPC acquired the ECA's fledgling labor projects as well as the accompanying funds. Foreign labor operations continued and became a major focus of CIA activity on a worldwide basis throughout the 1950's and into the mid-1960's.

The national elections in Europe in 1948 had been a primary motivation in the establishment of OPC. By channeling funds to center parties and developing media assets, OPC attempted to influence election results—with considerable success. These activities formed the basis for covert political action for the next twenty years. By 1952 approximately forty different covert action projects were underway in one central European country alone. Other projects were targeted against what was then referred to as the "Soviet bloc."

During his term in the State Department Wisner had spent much of his time on problems involving refugees in Germany, Austriaa and Trieste. In addition, his service with OSS had been oriented toward Central Europe. The combination of State's continuing interest and Wisner's personal experience led to OPC's immediate emphasis on Central European refugee operations. OPC representatives made contact with thousands of Soviet refugees and emigrés for the purpose of influencing their political leadership. The National Committee for Free Europe, a group of prominent American businessmen, lawyers, and philanthropists, and Radio Free Europe were products of the OPC program.

Until 1950 OPC's paramilitary activities (also referred to as preventive direct action) were limited to plans and preparations for stay-behind nets in the event of future war. Requested by the Joint Chiefs of Staff, these projected OPC operations focused, once again, on Western Europe and were designed to support NATO forces against Soviet attack.

---

[27] The Psychological Strategy Board (PSB) was an NSC subcommittee established on April 4, 1951 to exercise direction over psychological warfare programs. Its membership included departmental representatives and PSB staff members.

The outbreak of the Korean War significantly altered the nature of OPC's paramilitary activities as well as the organization's overall size and capability. Between fiscal year 1950 and fiscal year 1951, OPC's personnel strength jumped from 584 to 1531. Most of that growth took place in paramilitary activities in the Far East. In the summer of 1950, following the North Korean invasion of South Korea, the State Department requested the initiation of paramilitary and psychological operations on the Chinese mainland. Whatever MacArthur's preferences, the JCS were also eager for support activities in the Far East. This marked the beginning of OPC's active paramilitary engagement. The Korean War established OPC's and CIA's jurisdiction in the Far East and created the basic paramilitary capability that the Agency employed for twenty years. By 1953, the elements of that capability were "in place"—aircraft, amphibious craft, and an experienced group of personnel. For the next quarter century paramilitary activities remained the major CIA covert activity in the Far East.

E. OPC INTEGRATION AND THE OPC-OSO MERGER

The creation of OPC and its ambiguous relationship to the Agency precipitated two major administrative problems, the D'CI's relationship to OPC and antagonism between OPC and the Agency's clandestine collection component, the Office of Special Operations. DCI Walter Bedell Smith acted to rectify both problems.

As OPC continued to grow, Smith's predecessor, Admiral Hillenkoetter, resented the fact that he had no management authority over OPC, although its budget and personnel were being allocated through the CIA. Hillenkoetter's clashes with the State and Defense Departments as well as with Wisner, the Director of OPC, were frequent. Less than a week after taking office Smith announced that as DCI he would assume administrative control of OPC and that State and Defense would channel their policy guidance through him rather than through Wisner. On October 12, 1950, the representatives of State, Defense and the Joint Chiefs of Staff formally accepted the change. The ease with which the shift occurred was primarily a result of Smith's own position of influence with the Departments.

OPC's anomalous position in the Agency revealed the difficulty of maintaining two separate organizations for the execution of varying but overlapping clandestine activities. The close "tradecraft" relationship between clandestine collection and covert action, and the frequent necessity for one to support the other was totally distorted with the separation of functions in OSO and OPC. Organizational rivalry rather than interchange dominated the relationship between the two components.

On the operating level the conflicts were intense. Each component had representatives conducting separate operations at each station. Given the related missions of the two, OPC and OSO personnel were often competing for the same agents and, not infrequently, attempting to wrest agents from each other. In 1952 the outright hostility between the two organizations in Bangkok required the direct intervention of the Assistant Director for Special Operations, Lyman Kirkpatrick. There an important official was closely tied to OPC, and OSO was trying to lure him into its employ.

The OPC-OSO conflict was only partially the result of overseas competition for assets. Salary differentials and the differences in mission were other sources of antagonism. At the time of its creation in 1948 OPC was granted liberal funding to attract personnel quickly in order to get its operation underway. In addition, the burgeoning activities enabled people, once hired, to rise rapidly. The result was that OPC personnel held higher-ranking, better-paid positions, than their OSO counterparts.

Many OSO personnel had served with OSS, and their resentment of OPC was intensified by the fact that they regarded themselves as the intelligence "purists," the professionals who engaged in collection rather than action and whose prewar experience made them more knowledgeable and expert than the OPC recruits. In particular, OSO personnel regarded OPC's high-risk operations as a threat to the maintenance of OSO security and cover. OPC's favored position with State and Defense, its generous budget, and its visible accomplishments all contrasted sharply with OSO's silent, long-term objectives in espionage and counterespionage. By June 1952 OPC had overtaken OSO in personnel and budget allocation. Soon after his appointment as DCI, Smith addressed the problem of the OPC-OSO conflict. Lawrence Houston, the CIA's General Counsel, had raised the issue with him and recommended a merger of the two organizations.[28] Sentiment in OSO and OPC favored the principle of a merger. Lyman Kirkpatrick, the Executive Assistant to the DCI, Major General W. G. Wyman, Assistant Director for Special Operations, Wisner, and William Jackson all appeared to have favored a merger—although there was disagreement on the form it should take.

Between 1951 and 1952 Smith made several cosmetic changes to foster better coordination between OPC and OSO. Among them was the appointment of Allen W. Dulles as Deputy Director for Plans in January 1951.[29] Dulles was responsible for supervising both OPC and OSO, although the two components were independently administered by their own Directors. During this period of "benign coordination" Smith consulted extensively with senior officials in OPC and OSO. OPC's rapid growth and its institutional dynamism colored the attitude of OSO toward a potential merger. In the discussions which Bedell Smith held, senior OSO personnel, specifically Lyman Kirkpatrick and Richard Helms, argued for an integration of OPC functions under OSO control rather than an integrated chain of command down to station level. Fundamentally, the OSO leadership feared being engulfed by OPC in both operations and in personnel. However, by this time Bedell Smith was committed to the idea of an integrated structure.

Although some effort was made to combine the OSO and OPC Western Hemisphere Divisions in June 1951, real integration at the operations level did not occur until August 1952, when OSO and OPC became the Directorate of Plans (DDP). Under this arrangement, Wisner was named Deputy Director for Plans and assumed the command functions of the ADSO and ADPC. Wisner's second in command, Chief of Operations, was Richard Helms, drawn from the OSO side to strike a balance at the senior level. At this time Dulles replaced Jackson as DDCI.

The merger resulted in the maximum development of covert action over clandestine collection. There were several reasons for this. First was the orientation of Wisner himself. Wisner's OSS background and his OPC experience had established his interests in the operational side of clandestine activities. Second, for people in the field, rewards came more quickly through visible operational accomplishments than through the silent, long-term development of agents required for clandestine collection. In the words of one former high-ranking DDP official, "Collection is the hardest thing of all; it's much easier to plant an article in a local newspaper."

---

[28] The Dulles-Jackson-Correa survey had also advised a merger of OPC, OSO and the Office of Operations, the Agency's overt collection component.

[29] Dulles had been serving as an advisor to successive DCIs since 1947. Smith and Jackson prevailed upon him to join the Agency on a full-time basis.

F. CONGRESSIONAL REVIEW

The CIA was conceived and organized as an agent of the Executive branch. Traditionally, Congress' only formal relationship to the Agency was through the appropriations process. The concept of Congressional oversight in the sense of scrutinizing and being fully informed of Agency activities did not exist. The international atmosphere, Congress relationship to the Executive branch and the Congressional committee structure determined the pattern of interaction between the Agency and members of the legislature. Acceptance of the need for clandestine activities and of the need for secrecy to protect those activities contributed to Congress' relatively unquestioning and uncritical attitude regarding the CIA, as did the Executive branch's ascendancy in foreign policy for nearly two decades following World War II. The strong committee system which accorded enormous power to committee chairmen and limited the participation of less senior members in committee business resulted in informal arrangements whereby selected members were kept informed of Agency activities primarily through one-to-one exchanges with the DCI.

In 1946, following a Joint Committee review Congress enacted the Legislative Reorganization Act which reduced the number of committees and realigned their jurisdictions.[30] The prospect of a unified military establishment figured into the 1946 debates and decisions on Congressional reorganization. However, Congress did not anticipate having to deal with the CIA. This meant that after the passage of the National Security Act in 1947 CIA affairs had to be handled within a committee structure which had not accommodated itself to the existence of a central intelligence agency.

In the House and Senate the Armed Services and Appropriations Committees were granted jurisdiction over the Agency. No formal CIA subcommittees were organized until 1956. Until then small *ad hoc* groups composed of a few senior committee members reviewed the budget, appropriated funds, and received annual briefings on CIA activities. The DCIs kept senior committee members informed of large-scale covert action projects at the approximate time of implementation. There was no formal review or approval process involved; it was simply a matter of courtesy to the senior members. The initiative in gaining information on specific activities rested with the members.

For nearly twenty years a small group of ranking members dominated these relationships with the Agency. As Chairman of the House Armed Services Committee, Representative Carl Vinson, a Democrat from Georgia, presided over CIA matters from 1949 to 1953 and from 1955 to 1965. Clarence Cannon served as chairman of the House Appropriations Committee from 1949 to 1953 and from 1955 to 1964 and chaired the Defense Subcommittee which had supervising authority over CIA appropriations. Cannon organized a special group of five members to meet informally on CIA appropriations. In the Senate between 1947 and 1954 chairmanship of the Armed Services Committee was held by Chan Gurney, Millard Tydings, Richard Russell and Leverett Saltonstall. In 1955 Russell assumed the chairmanship and held the position until 1968.

Because the committee chairmen maintained their positions for extended periods of time, they established continuing relationships with DCIs and preserved an exclusivity in their knowledge of Agency activities. They were also able to develop relationships of

[30] The Act limited members' committee assignments, provided for professional staffing, tried to regularize meetings, and made some changes in the appropriations process as well as legislating other administrative modifications.

mutual trust and understanding with the DCIs which allowed informal exchanges to prevail over formal votes and close supervision.

Within the Congress procedures governing the Agency's budget assured maximum secrecy. The DCI presented his estimate of the budget for the coming fiscal year broken down into general functional categories. Certification by the subcommittee chairmen constituted approval. Exempt from floor debate and from public disclosure, CIA appropriations were and are concealed in the Department of Defense budget. In accordance with the 1949 Act the DCI has only to certify that the money as appropriated has been spent. He does not have to account publicly for specific expenditures, which would force him to reveal specific activities.

To allow greater flexibility for operational expenditures the Contingency Reserve Fund was created in 1952. The Fund provided a sum independent of the regular budget to be used for unanticipated large projects. For example, the initial funding for the development of the U-2 reconnaissance aircraft was drawn from the Contingency Reserve Fund. The most common use of the Fund was for covert operations.

Budgetary matters rather than the specific nature of CIA activities were the concern of Congressional members, and given the perception of the need for action against the Soviet Union, approval was routine. A former CIA Legislative Counsel characterized Congressional attitudes in the early 1950s in this way:

> In the view of the general public, and of the Congress which in the main reflected the public attitude, a national intelligence service in those days was more or less a part and parcel of our overall defense establishment. Therefore, as our defense budget went sailing through Congress under the impact of the Soviet extension of power into Eastern Europe, Soviet probes into Iran and Greece, the Berlin blockade, and eventually the Korean War, the relatively modest CIA budget in effect got a free ride, buried as it was in the Defense and other budgets. When Directors appeared before Congress, which they did only rarely, the main concern of the members was often to make sure that we [the CIA] had what we needed to do our job.

Limited information-sharing rather than rigorous oversight characterized Congress relationship to the Agency. Acceptance of the need for secrecy and Congressional procedures would perpetuate what amounted to mutual accommodation.

By 1953 the Agency had achieved the basic structure and scale it retained for the next twenty years.[30a] The Korean War, United States foreign policy objectives, and the Agency's internal organizational arrangements had combined to produce an enormous impetus for growth. The CIA was six times the size it had been in 1947.

Three Directorates had been established. In addition to the DDP and the DDI, Smith created the Deputy Directorate for Administration (DDA). Its purpose was to consolidate the management functions required for the burgeoning organization. The Directorate was responsible for budget, personnel, security, and medical services Agency-wide. However, one quarter of DDA's total personnel strength was assigned to logistical support for overseas operations. The DDP commanded the major share of the Agency's budget, personnel, and resources; in 1952 clandestine collection and covert action accounted for 74 percent of

[30a] For chart showing CIA organization as of 1953, see p. 98.

the Agency's total budget;[31] its personnel constituted 60 percent of the CIA's personnel strength. While production rather than coordination dominated the DDI, operational activities rather than collection dominated the DDP. The DDI and the DDP emerged at different times out of disparate policy needs. There were, in effect, separate organizations. These fundamental distinctions and emphases were reinforced in the next decade.

[31] This did not include DDA budgetary allocations in support of DDP operations.

APPENDIX B

THE HUGHES-RYAN ACT, 1974

Editor's note: The Hughes-Ryan Act, the first statutory tightening of controls over the CIA since the National Security Act of 1947, aimed at improving accountability for covert action through two steps: first, requiring that the president approve all important covert actions with a "finding" ("the president finds that each such operation is important") and, second, requiring that each finding be reported to lawmakers on the congressional Intelligence Committees. The law was passed on the last day of 1974, in the throes of the Watergate scandal and allegations that the CIA was involved in domestic spying and inappropriate covert actions against the democratically elected regime of President Salvador Allende of Chile.

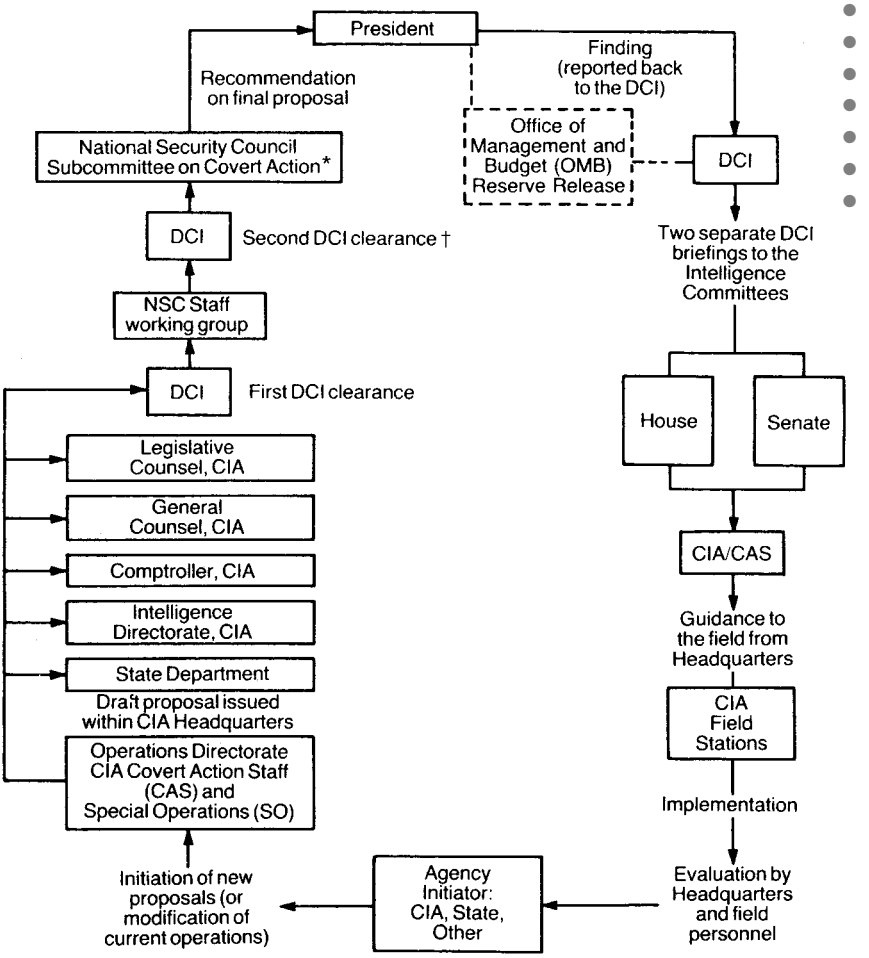
THE 1974 HUGHES-RYAN ACT

Also known as Section 662 (a) of the Foreign Assistance Act of 1974, the amendment states:

> No funds appropriated under the authority of this or any other Act may be expended by or on behalf of the Central Intelligence Agency for operations in foreign countries other than activities intended solely for obtaining necessary intelligence unless and until the President finds that each such operation is important to the national security of the United States and reports, in a timely fashion, a description and scope of each operation to the appropriate committees of Congress.

APPENDIX C

COVERT ACTION DECISION AND REPORTING PATHWAY



*Known as the Special Coordination Committee (SCC) during the Carter administration and the National Security Planning Group (NSPG) during the Reagan administration.

†Since 2005, the Director of National Intelligence (DNI) reveiws covert action proposals at this stage.

Editor's note: Since passage of the Hughes-Ryan Act in 1974, the pathway that a decision in favor of a covert action must follow is much more complicated than used to be the case. Before Hughes-Ryan, the Director of Central Intelligence (DCI) and the national security adviser would sometimes decide on covert actions without the involvement of anyone else, other than the intelligence officers and foreign assets engaged in the planning and implementation of the operation: no congressional involvement and often no presidential involvement. Now, as the diagram illustrates, covert actions must run a gauntlet of critics—valuable from the point of view of accountability, but, arguably, reducing efficiency and timeliness. Yet, as a staff intelligence overseer in the House of Representatives, the editor has seen this process take less than an hour in times of emergency, as a result of rapid and secure telephone conversations among the key participants in the review. The diagram presented here is from 1989 but remains valid today, except for the addition of another layer: the new Director of National Intelligence (replacing the DCI in 2005), placed between the NSC Staff working group and the NSC Subcommittee on Covert Action. One other related change: the Director of the Central Intelligence Agency (D/CIA) now provides the CIA's clearance before the proposal travels to the NSC Staff working group. The entry of the Department of Defense into the covert action domain is worrisome to many observers, who fear that the Hughes-Ryan checks on the wisdom of any particular covert action may be bypassed by the Pentagon, on grounds that the law applies to the CIA and not to the military—a dubious argument.

Source: Adapted from Loch K. Johnson, *America's Secret Power: The CIA in a Democratic Society* (New York: Oxford University Press, 1989), p. 113.

APPENDIX D

EXAMPLES OF PRESIDENTIAL FINDINGS FOR COVERT ACTION

Editor's note: The findings presented below were approved by President Ronald Reagan, the first regarding Central America on March 9, 1981, which received written approval; and the second regarding Iran on January 17, 1986, which received only an oral approval. Both were originally top secret, then declassified in the context of the congressional inquiry into the Iran-*contra* affair in 1987. Notice how in each instance, the "purpose" or "description" is succinct, leaving considerable leeway for the CIA to fill in the details during implementation of the covert action.

Example No. 1: Central America

> Finding Pursuant to Section 662 of the Foreign Assistance Act of 1961, As Amended, Concerning Operations Undertaken by the Central Intelligence Agency in Foreign Countries, Other Than Those Intended Solely for the Purpose of Intelligence Collection

I hereby find that the following operations in foreign countries (including all support necessary to such operations) are important to the national security of the United States, and direct the Director of Central Intelligence, or his designee, to report this Finding to the

---

Sources: *Public Papers of the President: Ronald Reagan* (Washington, DC: U.S. Government Printing Office, 1986); Presidential Finding on Central America, N16574; Iran Finding, 1/17/86, Hearings, Ex. JMP-29-D, *Report of the Congressional Committees Investigating the Iran-Contra Affair,* S. Rept. No. 100–216 and H. Rept. No. 100–433, 100th Cong., 1st Sess, U.S. Senate Select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition and U.S. House of Representatives Select Committee to Investigate Covert Arms Transactions with Iran (the Inouye-Hamilton Committee), November 1987.

concerned committees of the Congress pursuant to law, and to provide such briefings as necessary.

SCOPE	*PURPOSE*
Central America	Provide all forms of training, equipment and related assistance to cooperating governments throughout Central America in order to counter foreign-sponsored subversion and terrorism. [still-classified section missing here] Encourage and influence foreign governments around the world to support all of the above objectives.

Example No. 2: Iran

> Finding Pursuant to Section 662 of The Foreign Assistance Act of 1961 As Amended. Concerning Operations Undertaken by the Central Intelligence Agency in Foreign Countries. Other Than Those Intended Solely for the Purpose of Intelligence Collection

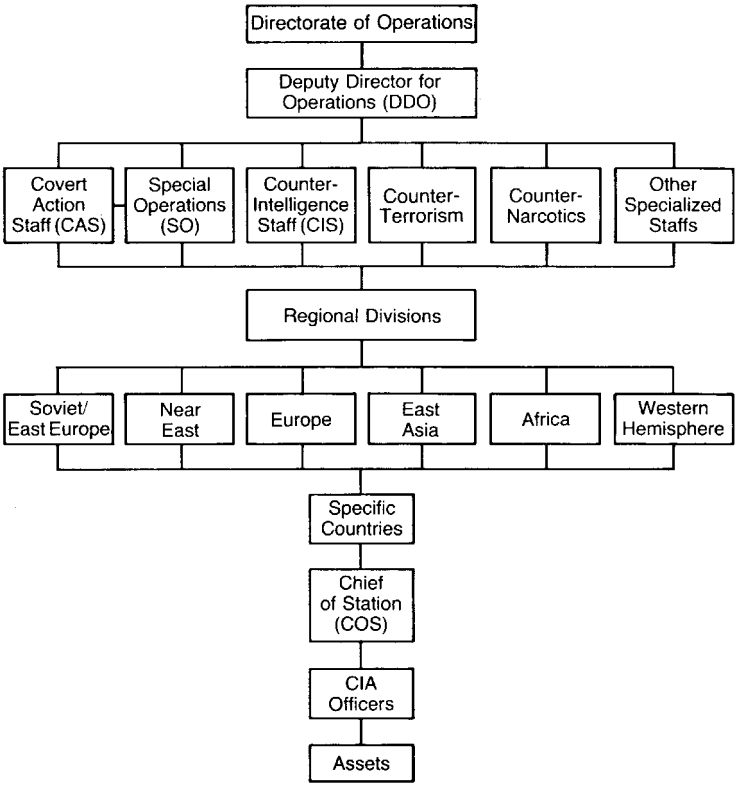
I hereby find that the following operation in a foreign country (including all support necessary to such operation) is important to the national security of the United States, and due to its extreme sensitivity and security risks. I determine it is essential to limit prior notice, and direct the Director of Central Intelligence to refrain from reporting this Finding to the Congress as provided in Section 501 of the National Security Act of 1947, as amended, until I otherwise direct.

SCOPE	*DESCRIPTION*
Iran	Assist selected friendly foreign liaison services, third countries and third parties which have established relationships with Iranian elements, groups, and individuals sympathetic to U.S. Government interests and which do not conduct or support terrorist actions directed against U.S. persons, property or interests, for the purpose of: (1) establishing a more moderate government in Iran, (2) obtaining from them significant intelligence not otherwise obtainable, determine the current Iranian Government's methods with respect to its neighbors and with respect to terrorist acts, and (3) furthering the release of the American hostages held in Beirut and preventing additional terrorist acts by these groups. Provide funds, intelligence, counter-intelligence, training, guidance and communications and other necessary assistance to these elements, groups, individuals, liaison services and third countries in support of these activities. The USG will act to facilitate efforts by third parties and third countries to establish contact with moderate elements within and outside the Government of Iran by providing these elements with arms, equipment and related material in order to enhance the credibility of these elements in their effort to achieve a more pro-U.S.

government in Iran by demonstrating their ability to obtain requisite resources to defend their country against Iraq and intervention by the Soviet Union. This support will be discontinued if the U.S. Government learns that these elements have abandoned their goals of moderating their government and appropriated the material for purposes other than that provided by this finding.

APPENDIX E

THE ORGANIZATION DURING THE COLD WAR OF THE CIA'S DIRECTORATE OF OPERATIONS—HOME BASE FOR COVERT OPERATIONS



Editor's note: The phrase "Special Operations" (SO) in the chart refers to paramilitary activities, a subset of covert action; the word "assets" refers to foreign nationals employed secretly by the CIA.

Source: Loch K. Johnson, *America's Secret Power: The CIA in a Democratic Society* (New York: Oxford University Press, 1989), p. 46.

APPENDIX F

THE CIA ASSASSINATION PLOT IN THE CONGO, 1960–61

III. ASSASSINATION PLANNING AND THE PLOTS

A. CONGO

1. Introduction

The Committee has received solid evidence of a plot to assassinate Patrice Lumumba. Strong hostility to Lumumba, voiced at the very highest levels of government may have been intended to initiate an assassination operation; at the least it engendered such an operation. The evidence indicates that it is likely that President Eisenhower's expression of strong concern about Lumumba at a meeting of the National Security Council on August 18, 1960, was taken by Allen Dulles as authority to assassinate Lumumba.[1] There is, however, testimony by Eisenhower Administration officials, and ambiguity and lack of clarity in the records of high-level policy meetings, which tends to contradict the evidence that the President intended an assassination effort against Lumumba.

The week after the August 18 NSC meeting, a presidential advisor reminded the Special Group of the "necessity for very straightforward action" against Lumumba and prompted a decision not to rule out consideration of "any particular kind of activity which might contribute to getting rid of Lumumba." The following day, Dulles cabled

---

Source: "Alleged Assassination Plots Involving Foreign Leaders," *An Interim Report,* Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee), U.S. Senate, 94th Cong., 2d Sess (1975), pp. 13–70.

[1] Indeed, one NSC staff member present at the August 18 meeting, believed that he witnessed a presidential order to assassinate Lumumba.

a CIA Station Officer in Leopoldville, Republic of the Congo,[2] that "in high quarters" the "removal" of Lumumba was "an urgent and prime objective." Shorty thereafter the CIA's clandestine service formulated a plot to assassinate Lumumba. The plot proceeded to the point that lethal substances and instruments specifically intended for use in an assassination were delivered by the CIA to the Congo Station. There is no evidence that these instruments of assassination were actually used against Lumumba.

A thread of historical background is necessary to weave these broad questions together with the documents and testimony received by the Committee.

In the summer of 1960, there was great concern at the highest levels in the United States government about the role of Patrice Lumumba in the Congo. Lumumba, who served briefly as Premier of the newly independent nation, was viewed with alarm by United States policymakers because of what they perceived as his magnetic public appeal and his leanings toward the Soviet Union.

Under the leadership of Lumumba and the new President, Joseph Kasavubu, the Congo declared its independence from Belgium on June 30, 1960.[3] In the turbulent month that followed, Lumumba threatened to invite Soviet troops to hasten the withdrawal of Belgian armed forces. The United Nations Security Council requested Belgium's withdrawal and dispatched a neutral force to the Congo to preserve order. In late July, Lumumba visited Washington and received pledges of economic aid from Secretary of State Christian Herter. By the beginning of September, Soviet airplanes, trucks, and technicians were arriving in the province where Lumumba's support was strongest.

In mid-September, after losing a struggle for the leadership of the government to Kasavubu and Joseph Mobutu, Chief of Staff of the Congolese armed forces, Lumumba sought protection from the United Nations forces in Leopoldville. Early in December, Mobutu's troops captured Lumumba while he was traveling toward his stronghold at Stanleyville and imprisoned him. On January 17, 1961, the central government of the Congo transferred Lumumba to the custody of authorities in Katanga province, which was then asserting its own independence from the Congo. Several weeks later, Katanga authorities announced Lumumba's death.

Accounts of the circumstances and timing of Lumumba's death vary. The United Nations investigation concluded that Lumumba was killed on January 17, 1961.[4]

---

[2] Since the period in which the events under examination occurred, the names of many geographical units and governmental institutions have changed. For instance, the nation formerly known as the Republic of the Congo is now the Republic of Zaire and the present capital city, Kinshasa, was known then as Leopoldville. For the sake of clarity in dealing with many of the documents involved in this section, the names used in this report are those which applied in the early 1960's.

[3] For detailed reporting of the events in the Congo during this period, see the *New York Times,* especially July 7, 1960, 7:3; July 14, 1960, 1:1; July 16, 1960, 1:1 and 3:2; July 28, 1960, 3:7; September 3, 1960, 3:2; September 6, 1960, 1:8; December 3, 1960, 1:8; January 18, 1961, 3:1; February 14, 1961, 1:1.

[4] Report of the Commission of Investigation. U.N. Security Council, Official Records, Supplement for October, November, and December, 11/11/61, p. 117. (Cited hereinafter as "U.N. Report, 11/11/61."

2. Dulles Cable to Leopoldville: August 26, 1960

The Congo declared its independence from Belgium on June 30, 1960. Shortly thereafter, the CIA assigned a new officer to its Leopoldville Station. The "Station Officer"[5] said that assassinating Lumumba was not discussed during his CIA briefings prior to departing for the Congo, nor during his brief return to Headquarters in connection with Lumumba's visit to Washington in late July. (Hedgman, 8/21/75, pp. 8–9)

During August, there was increasing concern about Lumumba's political strength in the Congo among the national security policymakers of the Eisenhower Administration.[6] This concern was nurtured by intelligence reports such as that cabled to CIA Headquarters by the Station Officer:

> EMBASSY AND STATION BELIEVE CONGO EXPERIENCING CLASSIC COMMUNIST EFFORT TAKEOVER GOVERNMENT. MANY FORCES AT WORK HERE: SOVIETS *** COMMUNIST PARTY, ETC. ALTHOUGH DIFFICULT DETERMINE MAJOR INFLUENCING FACTORS TO PREDICT OUTCOME STRUGGLE FOR POWER, DECISIVE PERIOD NOT FAR OFF. WHETHER OR NOT LUMUMBA ACTUALLY COMMIE OR JUST PLAYING COMMIE GAME TO ASSIST HIS SOLIDIFYING POWER, ANTI-WEST FORCES RAPIDLY INCREASING POWER CONGO AND THERE MAY BE LITTLE TIME LEFT IN WHICH TAKE ACTION TO AVOID ANOTHER CUBA. (CIA Cable, Leopoldville to Director, 8/18/60)

This cable stated the Station's operational "objective [of] replacing Lumumba with pro Western Group." Bronson Tweedy, who was Chief of the Africa Division of CIA's clandestine services, replied that he was seeking State Department approval for the proposed operation based upon "your and our belief Lumumba must be removed if possible." (CIA Cable, Tweedy to Leopoldville, 8/18/60) On August 19, DDP Richard Bissell, Director of CIA's covert operations branch, signed a follow-up cable to Leopoldville, saying: "You are authorized proceed with operation." (CIA Cable, Director to Leopoldville, 8/19/60)

Several days later, the Station Officer reported:

> ANTI-LUMUMBA LEADERS APPROACHED KASAVUBU WITH PLAN ASSASSINATE LUMUMBA *** KASAVUBU REFUSED AGREE SAYING HE RELUCTANT RESORT VIOLENCE AND NO OTHER LEADER SUFFICIENT STATURE REPLACE LUMUMBA. (CIA Cable, Leopoldville to Director, 8/24/60)

On August 25, Director of Central Intelligence, Allen Dulles attended a meeting of the Special Group—the National Security Council subcommittee responsible for the planning of covert operations.[7] In response to the outline of some CIA plans for political actions

---

[5] Victor Hedgman was one of the CIA officers in Leopoldville attached to the Congo Station and will be referred to hereinafter as "Station Officer."

[6] See Section 7, *infra,* for a full discussion of the prevailing anti-Lumumba attitude in the United States government as shown by minutes of the National Security Council and Special Group and the testimony of high Administration officials.

[7] The August 25th Special Group meeting and the testimony about its significance for the issue of authorization is discussed in detail in Section 7(a) (iii), *infra.*

That meeting was preceded by an NSC meeting on August 18, at which an NSC staff executive heard the President make a statement that impressed him as an order for the assassination of Lumumba. (Johnson, 6/18/75, pp. 6–7) The testimony about this NSC meeting is set forth in detail at Section 7 (a) (ii), *infra.*

against Lumumba, such as arranging a vote of no confidence by the Congolese Parliament, Gordon Gray, the Special Assistant to the President for National Security Affairs reported that the President "had expressed extremely strong feelings on the necessity for very straightforward action in this situation, and he wondered whether the plans as outlined were sufficient to accomplish this." (Special Group Minutes, 8/25/60) The Special Group "finally agreed that planning for the Congo would not necessarily rule out 'consideration' of any particular kind of activity which might contribute to getting rid of Lumumba." (Special Group Minutes, 8/25/60)

The next day, Allen Dulles signed a cable[8] to the Leopoldville Station Officer stating:

> IN HIGH QUARTERS HERE IT IS THE CLEAR-CUT CONCLUSION THAT IF [LUMUMBA] CONTINUES TO HOLD HIGH OFFICE, THE INEVITABLE RESULT WILL AT BEST BE CHAOS AND AT WORST PAVE THE WAY TO COMMUNIST TAKEOVER OF THE CONGO WITH DISASTROUS CONSEQUENCES FOR THE PRESTIGE OF THE UN AND FOR THE INTERESTS OF THE FREE WORLD GENERALLY. CONSEQUENTLY WE CONCLUDE THAT HIS REMOVAL MUST BE AN URGENT AND PRIME OBJECTIVE AND THAT UNDER EXISTING CONDITIONS THIS SHOULD BE A HIGH PRIORITY OF OUR COVERT ACTION. (CIA Cable, Dulles to Station Officer, 8/26/60)[9]

The cable said that the Station Officer was to be given "wider authority"—along the lines of the previously authorized operation to replace Lumumba with a pro-Western group—"including even more aggressive action if it can remain covert . . . we realize that targets of opportunity may present themselves to you." Dulles' cable also authorized the expenditure of up to $100,000 "to carry out any crash programs on which you do not have the opportunity to consult HQS," and assured the Station Officer that the message had been "seen and approved at competent level" in the State Department. (CIA Cable, 8/26/60) The cable continued:

> TO THE EXTENT THAT AMBASSADOR MAY DESIRE TO BE CONSULTED, YOU SHOULD SEEK HIS CONCURRENCE. IF IN ANY PARTICULAR CASE, HE DOES NOT WISH TO BE CONSULTED YOU CAN ACT ON YOUR OWN AUTHORITY WHERE TIME DOES NOT PERMIT REFERRAL HERE.

This cable raises the question of whether the DCI was contemplating action against Lumumba for which the United States would want to be in a position to "plausibly deny" responsibility. On its face, the cable could have been read as authorizing only the "removal" of Lumumba from office. DDP Richard Bissell was "almost certain" that he was informed about the Dulles cable shortly after its transmission. He testified that it was his

[8] Cables issued under the personal signature of the DCI are a relative rarity in CIA communications and call attention to the importance and sensitivity of the matter discusseed. By contrast, cable traffic to and from CIA field stations routinely refers to the sender or recipient as "Director" which simply denotes "CIA Headquarters."

[9] The bracketed words in cables throughout this section signify that a cryptonym, pseudonym, or other coded reference has been translated in order to maintain the security of CIA communications and to render the cable traffic comprehensible. The translations were provided to the Committee by the CIA Review Staff and by various witnesses.

"belief" that the cable was a circumlocutious means of indicating that the President wanted Lumumba killed.[10] (Bissell, 9/10/75, pp. 12, 33, 64–65)

Bronson Tweedy testified that he may have seen Dulles' cable of August 26, before it was transmitted and that he "might even have drafted it." Tweedy called this cable the "most authoritative statement" on the "policy consensus in Washington about the need for the removal of Lumumba" by any means, including assassination. He said that he "never knew" specifically who was involved in formulating this policy. But he believed that the cable indicated that Dulles had received authorization at the "policy level" which "certainly ∗∗∗ would have involved the National Security Council." Tweedy testified that the $100,000 was probably intended for "political operations against Lumumba ∗∗∗ not assassination-type programs." (Tweedy, 10/9/75 1, p. 5, II, pp. 5–7, 24, 26)

3. CIA Encouragement of Congolese Efforts to "Eliminate" Lumumba

On September 5, 1960, President Kasavubu dismissed Premier Lumumba from the government despite the strong support for Lumumba in the Congolese Parliament. After losing the ensuing power struggle with Kasavubu and Mobutu, who seized power by a military coup on September 14, Lumumba asked the United Nations peace-keeping force for protection.

The evidence indicates that the ouster of Lumumba did not alleviate the concern about him in the United States government. Rather, CIA and high Administration officials[11] continued to view him as a threat.

During this period, CIA officers in the Congo advised and aided Congolese contacts known to have an intent to assassinate Lumumba. The officers also urged the "permanent disposal" of Lumumba by some of these Congolese contacts. Moreover, the CIA opposed reopening Parliament after the coup because of the likelihood that Parliament would return Lumumba to power.

The day after Kasavubu deposed Lumumba, two CIA officers met with a high-level Congolese politician who was in close contact with the Leopoldville Station. The Station reported to CIA Headquarters:

> TO [STATION OFFICER] COMMENT THAT LUMUMBA IN OPPOSITION IS ALMOST AS DANGEROUS AS IN OFFICE, [THE CONGOLESE, POLITICIAN] INDICATED UNDERSTOOD AND IMPLIED MIGHT PHYSICALLY ELIMINATE LUMUMBA. (CIA Cable, Leopoldville to Director, 9/7/60)

The cable also stated that the Station Officer had offered to assist this politician "in preparation new government program" and assured him that the United States would supply technicians. (CIA Cable, 9/7/60)

As the struggle for power raged, Bronson Tweedy summarized the prevalent apprehension of the United States about Lumumba's ability to influence events in the Congo by virtue of his personality, irrespective of his official position:

---

[10] See Section 7(c), *infra* for additional testimony by Bissell on the question of authorization for the assassination effort against Lumumba. Bissell testified, *inter alia,* that Dulles would have used the phrase "highest quarters" to refer to the President.

[11] A detailed treatment of the expressions of continued concern over Lumumba at the National Security Council level is set forth in Section 7, *infra.*

> LUMUMBA TALENTS AND DYNAMISM APPEAR OVERRIDING FACTOR IN RE-ESTABLISHING HIS POSITION EACH TIME IT SEEMS HALF LOST. IN OTHER WORDS EACH TIME LUMUMBA HAS OPPORTUNITY HAVE LAST WORD HE CAN SWAY EVENTS TO HIS ADVANTAGE. (CIA Cable, Director to Leopoldville, 9/13/60)

The day after Mobutu's coup, the Station Officer reported that he was serving as an advisor to a Congolese effort to "eliminate" Lumumba due to his "fear" that Lumumba might, in fact, have been strengthened by placing himself in U.N. custody, which afforded a safe base of operations. Hedginan concluded: "Only solution is remove him from scene soonest." (CIA Cable, Leopoldville to Director, 9/15/60)

On September 17, another CIA operative in the Congo met with a leading Congolese senator. The cable to CIA Headquarters concerning the meeting reported:

> [CONGOLESE SENATOR] REQUESTED CLANDESTINE SUPPLY SMALL ARMS TO EQUIP *** TROOPS RECENTLY ARRIVED [LEOPOLDVILLE] AREA *** [THE SENATOR] SAYS THIS WOULD PROVIDE CORE ARMED MEN WILLING AND ABLE TAKE DIRECT ACTION *** [SENATOR] RELUCTANTLY AGREES LUMUMBA MUST GO PERMANENTLY. DISTRUSTS [ANOTHER CONGOLESE LEADER] BUT WILLING MAKE PEACE WITH HIM FOR PURPOSES ELIMINATION LUMUMBA. (CIA Cable, Leopoldville to Director, 9/17/60)

The CIA operative told the Congolese senator that, "he would explore possibility obtaining arms" and he recommended to CIA headquarters that they should:

> HAVE [ARMS] SUPPLIES READY TO GO AT NEAREST BASE PENDING [UNITED STATES] DECISION THAT SUPPLY WARRANTED AND NECESSARY. (CIA Cable, 9/17/60)[12]

Several days later, the Station Officer warned a key Congolese leader about coup plots led by Lumumba and two of his supporters, and: "Urged arrest or other more permanent disposal of Lumumba, Gizenga, and Mulele." (CIA Cable, Leopoldville to Director, 9/20/61) Gizenga and Mulele Were Lumumba's lieutenants who led his supporters while Lumumba was in U.N. custody.

---

[12] This recommendation proved to be in line with large scale planning at CIA Headquarters for clandestine paramilitary support to anti-Lumumba elements. On October 6, 1960, Richard Bissell and Bronson Tweedy signed a cable concerning plans which the Station Officer was instructed not to discuss with State Department representatives or operational contacts:

> [IN] VIEW UNCERTAIN OUTCOME CURRENT DEVELOPMENTS [CIA] CONDUCTING CONTINGENCY PLANNING FOR CONGO AT REQUEST POLICY ECHELONS. THIS PLANNING DESIGNED TO PREPARE FOR SITUATION IN WAY [UNITED STATES] WOULD PROVIDE CLANDESTINE SUPPORT TO ELEMENTS IN ARMED OPPOSITION TO LUMUMBA. CONTEMPLATED ACTION INCLUDES PROVISION ARMS, SUPPLIES AND PERHAPS SOME TRAINING TO ANTI-LUMUMBA RESISTANCE GROUPS. (CIA Cable, Director in Leopoldville, 10/6/60)

Throughout the fall of 1960, while Lumumba remained in U.N. protective custody,[13] the CIA continued to view him as a serious political threat. One concern was that if Parliament were re-opened and the moderates failed to obtain a majority vote, the "pressures for [Lumumba's] return will be almost irresistible." (CIA Cable, Leopoldville to Director, 10/26/60).[14] Another concern at CIA Headquarters was that foreign powers would intervene in the Congo and bring Lumumba to power. (CIA Cable, Director to Leopoldville, 10/17/60) Lumumba was also viewed by the CIA and the Administration as a stalking horse for "what appeared to be a Soviet effort to take over the Congo." (Hedgman, 8/21/75, pp. 10, 45)[15]

After Lumumba was in U.N. custody, the Leopoldville Station continued to maintain close contact with Congolese who expressed a desire to assassinate Lumumba.[16] CIA officers encouraged and offered to aid these Congolese in their efforts against Lumumba, although there is no evidence that aid was ever provided for the specific purpose of assassination.

4. The Plot to Assassinate Lumumba

SUMMARY

In the Summer of 1960, DDP Richard Bissell asked the Chief of the Africa Division, Bronson Tweedy, to explore the feasibility of assassinating Patrice Lumumba. Bissell also asked a CIA scientist, Joseph Scheider, to make preparations to assassinate or incapacitate an unspecified "African leader." According to Scheider, Bissell said that the assignment

---

[13] Both Richard Bissell and Bronson Tweedy confirmed that the CIA continued to view Lumumba as a threat even after he placed himself in U.N. custody. (Bissell, 9/10/75, pp. 68–69, 79: Tweedy, 9/9/75, pp. 48–50) Two factors were mentioned consistently in testimony by government officials to substantiate this view: first, Lumumba was a spellbinding orator with the ability to stir masses of people to action; and second, the U.N. forces did not restrain Lumumba's freedom of movement and the Congolese army surrounding them were often lax in maintaining their vigil. (Mulroney, 9/11/75, pp. 22–24; Dillon, 9/2/75. p. 49) As CIA officer Michael J. Mulroney put it, the fact that Lumumba was in United Nations custody "did not result in a cessation of his political activity." (Mulroney, 9/11/75, p. 23)

[14] A CIA Cable from Leopoldville to the Director on November 3, 1960 returned to this theme: the opening of the Congolese Parliament by the United Nations is opposed because it "WOULD PROBABLY RETURN LUMUMBA TO POWER."

[15] See Section 7, *infra*, for a treatment of the expression of this viewpoint at high-level policy meetings.

Tweedy expressed an even broader "domino theory" about the impact of Lumumba's leadership in the Congo upon events in the rest of Africa:

"The concern with Lumumba was not really the concern with Lumumba as a person. It was concern at this very pregnant point in the new African development [with] the effect on the balance of the Continent of a disintegration of the Congo. [I]t was the general feeling that Lumumba had it within his power to bring about this dissolution, and this was the fear that it would merely be the start—the Congo, after all, was the largest geographical expression. Contained in it were enormously important mineral resources ∗∗∗. The Congo itself, is adjacent to Nigeria, which at that point was considered to be one of the main hopes of the future stability of Africa. [I]f the Congo had fallen, then the chances were Nigeria would be seized with the same infection.

"This was why Washington ∗∗∗ was so concerned about Lumumba, not because there was something unique about Lumumba, but it was the Congo." (Tweedy. 10/9/75 II. p. 42)

[16] A Congolese in contact with the CIA "IMPLIED HE TRYING HAVE [LUMUMBA] KILLED BUT ADDED THIS MOST DIFFICULT AS JOB WOULD HAVE BE DONE BY AFRICAN WITH NO APPARENT INVOLVEMENT WHITE MAN." (CIA Cable, Leopoldville to Director, 10/28S/60)

had the "highest authority." Scheider procured toxic biological materials in response to Bissell's request, and was then ordered by Tweedy to take these materials to the Station Officer in Leopoldville. According to Scheider, there was no explicit requirement that the Station check back with Headquarters for final approval before proceeding to assassinate Lumumba. Tweedy maintained, however, that whether or not he had explicitly levied such a requirement, the Station Officer was not authorized to move from exploring means of assassination to actually attempting to kill Lumumba without referring the matter to Headquarters for a policy decision.

In late September, Scheider delivered the lethal substances to the Station Officer in Leopoldville and instructed him to assassinate Patrice Lumumba. The Station Officer testified that after requesting and receiving confirmation from CIA Headquarters that he was to carry out Scheider's instructions, he proceeded to take "exploratory steps" in furtherance of the assassination plot. The Station Officer also testified that he was told by Scheider that President Eisenhower had ordered the assassination of Lumumba. Scheider's testimony generally substantiated this account, although he acknowledged that his meetings with Bissell and Tweedy were the only bases for his impression about Presidential authorization. Scheider's mission to the Congo was preceded and followed by cables from Headquarters urging the "elimination" of Lumumba transmitted through an extraordinarily restricted "Eyes Only" channel—including two messages bearing the personal signature of Allen Dulles.

The toxic substances were never used. But there is no evidence that the assassination operation was terminated before Lumumba's death. There is, however, no suggestion of a connection between the assassination plot and the events which actually led to Lumumba's death.[17]

(a) Bissell/Tweedy Meetings on Feasibility of Assassinating Lumumba

Bronson Tweedy testified that Richard Bissell initiated a discussion with him in the summer of 1960 about the feasibility of assassinating Patrice Lumumba, and that they discussed the subject "more than once" during the following fall. Tweedy said the first such conversation probably took place shortly before Dulles' cable of August 26, instructing the Station Officer that Lumumba's "removal" was a "high priority of our covert action."[18] Whether his talk with Bissell was "shortly before or shortly after" the Dulles cable, it was clear to Tweedy that the two events "were totally in tandem." (Tweedy, 9/9/75, pp. 14–15; 10/9/75 II, p. 6)

Tweedy testified that he did not recall the exact exchange but the point of the conversation was clear:

What Mr. Bissell was saying to me was that there was agreement, policy agreement, in Washington that Lumumba must be removed from the position of control and influence in the Congo * * * and that among the possibilities of that elimination was indeed assassination.

* * * The purpose of his conversation with me was to initiate correspondence with the Station for them to explore with Headquarters the possibility of * * * assassination, or indeed any other means of removing Lumumba from power * * * to have the Station start reviewing possibilities, assets, and discussing them with Headquarters in detail in the same way we would with any operation. (Tweedy, 10/9/75 II, pp. 6, 8)

---

[17] See Section 6, *infra*, for a discussion of the evidence about the circumstances surrounding Lumumba's death in Katanga.

[18] See Section 2, *supra*.

Tweedy was "sure" that in his discussions with Bissell poisoning "must have" been mentioned as one means of assassination that was being considered and which the Station Officer should explore. (Tweedy, 9/9/75, pp. 26–27)

Tweedy testified that Bissell assigned him the task of working out the "operational details," such as assessing possible agents and the security of the operation, and of finding "some solution that looked as if it made sense, and had a promise of success." Tweedy stated that Bissell "never said ∗∗∗ go ahead and do it in your own good time without any further reference to me." Rather, Tweedy operated under the impression that if a feasible means of assassinating Lumumba were developed, the decision on proceeding with an assassination attempt was to be referred to Bissell. (Tweedy, 10/9/75 I, pp. 7, 17–18)

Tweedy stated that he did not know whether Bissell had consulted with any "higher authority" about exploring the possibilities for assassinating Lumumba. Tweedy said, that generally, when he received an instruction from Bissell:

I would proceed with it on the basis that he was authorized to give me instructions and it was up to him to bloody well know what he was empowered to tell me to do. (Tweedy, 9/9/75, p. 13)[19]

(b) Bissell/Scheider Meetings on Preparations for Assassinating "An African Leader"

Joseph Scheider[20] testified that he had "two or three conversations" with Richard Bissell in 1960 about the Agency's technical capability to assassinate foreign leaders. In the late spring or early summer, Bissell asked Scheider generally about technical means of assassination or incapacitation that could be developed or procured by the CIA. Scheider informed Bissell that the CIA had access to lethal or potentially lethal biological materials that could be used in this manner. Following their initial "general discussion," Scheider said he discussed assassination capabilities with Bissell in the context of "one or two meetings about Africa." (Scheider, 10/7/75, pp. 6–7, 41)

Scheider testified that in the late summer or early fall, Bissell asked him to make all preparations necessary for having biological materials ready on short notice for use in the assassination of an unspecified African leader, "in case the decision was to go ahead."[21]

---

[19] When asked whether he considered declining Bissell's assignment to move toward the assassination of Lumumba, Tweedy responded:

TWEEDY: I certainly did not attempt to decline it, and I felt, in view of the position of the government on the thing, that at least the exploration of this, or possibility of removing Lumumba from power in the Congo was an objective worth pursuing.

Q: Including killing him?

TWEEDY: Yes. I suspect I was ready to consider this ∗∗∗ Getting rid of him was an objective worth pursuing, and if the government and my betters wished to pursue it, professionally, I was perfectly willing to play my role in it, yes ∗∗∗. Having to do it all over again, it would be my strong recommendation that we not get into it. (Tweedy, 10/9/75, II, pp. 39–41)

[20] During the events discussed in the Lumumba case, Joseph Scheider served as Special Assistant to the DDP (Bissell) for Scientific Matters. Scheider holds a degree in bio-organic chemistry. (Scheider, 10/7/75, pp. 13, 25–29)

[21] Scheider said it was possible that Bissell subsequently gave him the "go signal" for his trip to the Congo and specified Lumumba as the target of the assassination operation. (Scheider, 10/7/75, pp. 65, 113–114; 10/7/75, p. 8) Scheider had a clearer memory, however, of another meeting, where the top officers of CIA's Africa Division, acting under Bissell's authority, actually dispatched to the Congo. (See Section 4(c), *infra*)

Scheider testified that Bissell told him that "he had direction from the highest authority ∗ ∗ ∗ for getting into that kind of operation." Scheider stated that the reference to "highest authority" by Bissell "signified to me that he meant the President."[22] (Scheider, 10/7/75, pp. 51–55, 58; 10/9/75, p. 8)

Scheider said that he "must have" outlined to Bissell the steps he planned to take to execute Bissell's orders. (Scheider, 10/7/75, p. 58) After the meeting, Scheider reviewed a list of biological materials available at the Army Chemical Corps installation at Fort Detrick, Maryland which would produce diseases that would "either kill the individual or incapacitate him so severely that he would be out of action." (Scheider, 10/7/75, pp. 63–64; 10/9/75, pp. 8–9, 12)[23] Scheider selected one material from the list which "was supposed to produce a disease that was ∗ ∗ ∗ indigenous to that area [of Africa] and that could be fatal." (Scheider, 10/7/75, p. 63) Scheider testified that he obtained this material and made preparation for its use:

> We had to get it bottled and packaged in a way that it could pass for something else and I needed to have a second material that could absolutely inactivate it in case that is what I desired to do for some contingency. (Scheider, 10/7/75, p. 64)

Scheider also "prepared a packet of ∗ ∗ ∗ accessory materials," such as hypodermic needles, rubber gloves, and gauze masks, "that would be used in the handling of this pretty dangerous material." (Scheider, 10/7/75, p. 59)

(c) Scheider Mission to the Congo on an Assassination Operation

Scheider testified that he remembered "very clearly" a conversation with Tweedy and the Deputy Chief of the Africa Division in September 1960 which "triggered" his trip to the Congo after he had prepared toxic biological materials and accessories for use in an assassination operation. (Scheider, 10/7/75, pp. 41, 65) According to Scheider, Tweedy and his Deputy asked him to take the toxic materials to the Congo and deliver instructions from Headquarters to the Station Officer: "to mount an operation, if he could do it securely ∗ ∗ ∗ to either seriously incapacitate or eliminate Lumumba." (Scheider, 10/7/75, p. 66)

Scheider said that he was directed to provide technical support to the Station Officer's attempt to find a feasible means of carrying out the assassination operation:

> They urged me to be sure that ∗ ∗ ∗ if these technical materials were used ∗ ∗ ∗ I was to make the technical judgments if there were any reasons the things shouldn't go, that was my responsibility. (Scheider, 10/7/75, p. 68)[24]

---

[22] See Section 7(d), *infra* for additional testimony by Scheider about the question of Presidential authorization for the assassination of Lumumba.

[23] Schieder said that there were "seven or eight materials" on the list, including tularemia ("rabbit fever"), brucellosis (undulant fever), tuberculosis, anthrax, smallpox, and Venezuelan equine encephalitis ("sleeping sickness"). (Scheider, 10/7/75, p. 64; 10/9/75, p. 9)

[24] When asked if he had considered declining to undertake the assignment to provide technical support to an assassination operation, Scheider stated:

"I think that my view of the job at the time and the responsibilities I had was in the context of a silent war that was being waged, although I realize that one of my stances could have been ∗ ∗ ∗ as a conscientious objector to this war. That was not my view. I felt that a decision had been made ∗ ∗ ∗ at the highest level that this be done and that as unpleasant a responsibility as it was, it was my responsibility to carry out my part of that." (Scheider, 10/9/75, p. 63)

According to Scheider, the Station Officer was to be responsible for "the operations aspects, what assets to use and other non-technical considerations." Scheider said that in the course of directing him to carry instructions to the Station Officer in the Congo, Tweedy and his Deputy "referred to the previous conversation I had with Bissell," and left Scheider with, "the impression that Bissell's statements to me in our previous meeting held and that they were carrying this message from Bissell to me." (Scheider, 10/9/75, pp. 13, 15, 69)

Although he did not have a specific recollection, Scheider stated that it was "probable" that he would have "checked with Bissell" to validate the extraordinary assignment he received from Tweedy and his Deputy, if indeed he had not actually received the initial assignment itself from Bissell. (Scheider, 10/7/75, pp. 113–114)

After being informed of Scheider's testimony about their meeting, and reviewing the contemporaneous cable traffic, Tweedy stated that it was "perfectly clear" that he had met with Scheider. He assumed that he had ordered Scheider to deliver lethal materials to the Leopoldville Station Officer and to serve as a technical adviser to the Station Officer's attempts to find a feasible means of assassinating Lumumba. (Tweedy, 10/9/75 I, pp. 18–21; 10/9/75 II, p. 9)

Tweedy said that his Deputy Chief was the only other person in the Africa Division who would have known that the assassination of Lumumba was being considered. (Tweedy, 9/9/75. p. 64) Tweedy assumed Scheider had "already been given his marching orders to go to the Congo by Mr. Bissell, not by me." (Tweedy, 10/9/75 II, p. 11)

Scheider testified that he departed for the Congo within a week of his meeting with Tweedy and his Deputy (Scheider, 10/9/75, p. 15)

(d) Congo Station Officer Told To Expect Scheider: Dulles Cables About "Elimination" of Lumumba

On September 19, 1960, several days after Lumumba placed himself in the protective custody of the United Nations peacekeeping force in Leopoldville, Richard Bissell and Bronson Tweedy sent a cryptic cable to Leopoldville to arrange a clandestine meeting between the Station Officer and "Joseph Braun," who was traveling to the Congo on an unspecified assignment. Joseph Scheider testified that "Joseph Braun" was his alias and was used because this was "an extremely sensitive operation." (Scheider, 10/7/75, pp. 78, 80) The cable informed the Station Officer:

> ["JOE"] SHOULD ARRIVE APPROX 27 SEPT * * * WILL ANNOUNCE HIMSELF AS "JOE FROM PARIS" * * * IT URGENT YOU SHOULD SEE ["JOE"] SOONEST POSSIBLE AFTER HE PHONES YOU. HE WILL FULLY IDENTIFY HIMSELF AND EXPLAIN HIS ASSIGNMENT TO YOU. (CIA Cable, Bissell, Tweedy to the Station Officer, 9/19/60)

The cable bore the codeword "PROP," which indicated extraordinary sensitivity and restricted circulation at CIA headquarters to Dulles, Bissell, Tweedy, and Tweedy's Deputy. The PROP designator restricted circulation in the Congo to the Station Officer. (Tweedy, 10/9/75 I, pp. 14–15; II, pp. 9, 37)

Tweedy testified that the PROP channel was established and used exclusively for the assassination operation. (Tweedy, 10/9/75 II, p. 37; 10/9/75 I, pp. 48–49) The Bissell/Tweedy cable informed the Station Officer that the PROP channel was to be used for:

> ALL [CABLE] TRAFFIC THIS OP, WHICH YOU INSTRUCTED HOLD ENTIRELY TO YOURSELF. (CIA Cable, 9/19/60)

Tweedy testified that the fact that he and Bissell both signed the cable indicated that authorization for Scheider's trip to the Congo had come from Bissell. Tweedy stated that Bissell "signed off" on cables originated by a Division Chief "on matters of particular sensitivity or so important that the DDP wished to be constantly informed about correspondence." Tweedy said that Bissell read much of the cable traffic on this operation and was "generally briefed on the progress of the planning." (Tweedy, 10/9/75 I, pp. 14, 54)

The Station Officer, Victor Hedgman testified to a clear, independent recollection of receiving the Tweedy/Bissell cable. He stated that in September of 1960 he received a "most unusual" cable from CIA Headquarters which advised that:

> someone who I would have recognized would arrive with instructions for me ∗∗∗ I believe the message was also marked for my eyes only ∗∗∗ and contained instructions that I was not to discuss the message with anyone.

He said that the cable did not specify the kind of instructions he was to receive, and it "did not refer to Lumumba in any way." (Hedgman, 8/21/75, pp. 11–13, 43)

Three days after the Bissell/Tweedy cable, Tweedy sent another cable through the PROP channel which stated that if it was decided that "support for prop objectives [was] essential" a third country national should be used as an agent in the assassination operation to completely conceal the American role.[25] (CIA Cable, 9/22/60) Tweedy testified that "PROP objectives" referred to an assassination attempt. (Tweedy, 10/9/75 I, p. 30) Tweedy also indicated to the Station Officer and his "colleague" Scheider:

> YOU AND COLLEAGUE[26] UNDERSTAND WE CANNOT READ OVER YOUR SHOULDER AS YOU PLAN AND ASSESS OPPORTUNITIES. OUR PRIMARY CONCERN MUST BE CONCEALMENT [AMERICAN] ROLE, UNLESS OUTSTANDING OPPORTUNITY EMERGES WHICH MAKES CALCULATED RISK FIRST CLASS BET. READY ENTERTAIN ANY SERIOUS PROPOSALS YOU MAKE BASED OUR HIGH REGARD BOTH YOUR PROFESSIONAL JUDGMENTS. (CIA Cable, 9/22/60)

On September 24, the DCI personally sent a cable to Leopoldville stating:

> WE WISH GIVE EVERY POSSIBLE SUPPORT IN ELIMINATING LUMUMBA FROM ANY POSSIBILITY RESUMING GOVERNMENTAL POSITION OR IF HE FAILS IN LEOPOLDVILLE, SETTING HIMSELF IN STANLEYVILLE OR ELSEWHERE. (CIA Cable, Dulles to Leopoldville, 9/24/60)

Dulles had expressed a similar view three days before in President Eisenhower's presence at an NSC meeting.[27]

---

[25] Tweedy also expressed reservations about two agents that the Station Officer was considering for this operation and said "WE ARE CONSIDERING A THIRD NATIONAL CUTOUT CONTACT CANDIDATE AVAILABLE HERE WHO MIGHT FILL BILL." (CIA Cable, 9/22/60) This is probably a reference to agent OJ/WIN, who was later dispatched to the Congo. His mission is discussed in Sections 5(b)–5(c), *infra*.

[26] Tweedy identified Scheider as the "colleague" referred to in this cable. (Tweedy, 10/9/75 I, p. 32) Scheider was en route to the Congo at this point.

[27] Dulles' statement at the NSC meeting of September 21, 1960 is discussed in detail at Section 7(a)(v), *infra.*

Scheider recalled that Tweedy and his Deputy had told him that the Station Officer would receive a communication assuring him that there was support at CIA Headquarters for the assignment Scheider was to give him. (Scheider, 10/7/75, pp. 88–90)

(e) Assassination Instructions Issued to Station Officer and Lethal Substances Delivered: September 26, 1960

Station Officer Hedgman reported through the PROP channel that he had contacted Scheider on September 26. (CIA Cable, Leopoldville to Tweedy, 9/27/60)

According to Hedgman:

HEDGMAN: It is my recollection that he advised me, or my instructions were, to eliminate Lumumba.

Q: By eliminate, do you mean assassinate?

HEDGMAN: Yes, I would say that was * * * my understanding of the primary means. I don't think it was probably limited to that, if there was some other way of * * * removing him from a position of political threat. (Hedgman, 8/21/75, pp. 17–18)

Hedgman said that he and Scheider also may have discussed non-lethal means of removing Lumumba as a "political threat," but he could not "recall with certainty on that." (Hedgman, 8/21/75, p. 28)

Scheider testified:

> I explained to him [Station Officer] what Tweedy and his Deputy had told me, that Headquarters wanted him to see if he could use this [biological] capability I brought against Lumumba [and] to caution him that it had to be done * * * without attribution to the USA. (Scheider, 10/9/75, p. 16)

The Station Officer testified that he received "rubber gloves, a mask, and a syringe" along with lethal biological material from Scheider, who also instructed him in their use.[28] Hedgman indicated that this paraphernalia was for administering the poison to Lumumba for the purpose of assassination. (Hedgman, 8/21/75, pp. 18–21, 24) Scheider explained that the toxic material was to be injected into some substance that Lumumba would ingest: "it had to do with anything he could get to his mouth, whether it was food or a toothbrush, * * * [so] that some of the material could get to his mouth." (Scheider, 10/7/75, p. 100)

Hedgman said that the means of assassination was not restricted to use of the toxic material provided by Scheider. (Hedgman, 8/21/75, p. 19)

He testified that he may have "suggested" shooting Lumumba to Scheider as an alternative to poisoning. (Hedgman, 8/21/75, pp. 19, 27–29) Scheider said it was his "impression" that Tweedy and his Deputy empowered him to tell the Station Officer that he could pursue other means of assassination. (Scheider, 10/7/75, pp. 100–101) Station Officer Hedgman testified that, although the selection of a mode of assassination was left to his judgment, there was a firm requirement that:

---

[28] Scheider testified that he sent the medical paraphernalia via diplomatic pouch. (Schelder, 10/7/75, pp. 59, 99)

> [I]f I implemented these instructions ∗ ∗ ∗ it had to be a way which could not be traced back ∗ ∗ ∗ either to an American or the United States government. (Hedgman, 8/21/75, p. 19)

Hedgman said Scheider assured him that the poisons were produced to: [leave] normal traces found in people that die of certain diseases." (Hedgman, 8/21/75, p. 23.)

Hedgman said that he had an "emotional reaction of great surprise" when it first became clear that Scheider had come to discuss an assassination plan. (Hedgman, 8/21/75, p. 30) He told Scheider he "would explore this." (Hedgman, 8/21/75, p. 46) and left Scheider with the impression "that I was going to look into it and try and figure if there was a way ∗ ∗ ∗ I believe I stressed the difficulty of trying to carry out such an operation." (Hedgman, 8/21/75, p. 47) Scheider said that the Station Officer was "sober [and] grim" but willing to proceed with the operation. (Scheider, 10/7/75, pp. 98, 121)

The Station Officer's report of his initial contact with Scheider was clearly an affirmative response to the assignment, and said that he and Scheider were "on same wavelength." (CIA Cable, Leopoldville to Tweedy, 9/27/60) Hedgman was "afraid" that the central government was "weakening under" foreign pressure to effect a reconciliation with Lumumba, and said:

> HENCE BELIEVE MOST RAPID ACTION CONSISTENT WITH SECURITY INDICATED. (CIA Cable, 9/27/60)[29]

(f) Hedgman's Impression That President Eisenhower Ordered Lumumba's Assassination

Station Officer Hedgman testified that Scheider indicated to him that President Eisenhower had authorized the assassination of Lumumba.[30] Hedgman had a "quite strong recollection" of asking about the source of authority for the assignment:

> HEDGMAN: I must have ∗ ∗ ∗ pointed out that this was not a common or usual Agency tactic ∗ ∗ ∗ never in my training or previous work in the Agency had I ever heard any references to such methods. And it is my recollection I asked on whose authority these instructions were issued.
>
> Q: And what did Mr. Scheider reply?
>
> HEDGMAN: It is my recollection that he identified the President ∗ ∗ ∗ and I cannot recall whether he said "the President," or whether he identified him by name. (Hedgman, 8/21/75, pp. 30–31)

Hedgman explained that Scheider told him "something to the effect that the President had instructed the Director" to assassinate Lumumba. (Hedgman, 8/21/75, pp. 32, 34)

Scheider stated that he had an "independent recollection" of telling the Station Officer about his meetings with Bissell, Tweedy, and Tweedy's Deputy, including Bissell's reference to "the highest authority." (Scheider, 10/7/75, p. 102) Scheider believed that he left

---

[29] Scheider interpreted this cable to mean that Hedgman was informing Headquarters: "that he has talked to me and that he is going to go ahead and see if he could mount the operation ∗ ∗ ∗ [H]e believes we ought to do it, if it is going to be done, as quickly as we can." (Scheider, 10/7/75, p. 121)

[30] See Section 7(d), *infra,* for a more detailed treatment of the testimony of the Station Officer and Scheider on the question of Presidential authorization for the assassination of Lumumba.

the Station Officer with the impression that there was presidential authorization for an assassination attempt against Lumumba. (Scheider, 10/7/75, pp. 90, 102–103)

(g) Steps in Furtherance of the Assassination Operation

(i) Hedgman's Testimony About Confirmation From Headquarters of the Assassination Plan.

Hedgman's testimony, taken fifteen years after the events in question and without the benefit of reviewing the cables discussed above, was compatible with the picture presented by the cables of a fully authorized and tightly restricted assassination operation. The only variance is that the cables portray Hedgman as taking an affirmative, aggressive attitude toward the assignment, while he testified that his pursuit of the operation was less vigorous.

The Station Officer testified that soon after cabling his request for confirmation that he was to carry out the assassination assignment, he received a reply from Headquarters, which he characterized as follows:

> I believe I received a reply which I interpreted to mean yes, that he was the messenger and his instructions were ∗∗∗ duly authorized. (Hedgman, 8/21/75, pp. 37–38)

Despite the cryptic nature of the cables, Hedgman said "I was convinced that yes, it was right," but he had no "desire to carry out these instructions." (Hedgman, 8/21/75, pp. 44, 50, 106) Hedgman stated:

> "I think probably that I would have gone back and advised that I intended to carry out and sought final approval before carrying it out had I been going to do it, had there been a way to do it. I did not see it as ∗∗∗ a matter which could be accomplished practically, certainly. (Hedgman, 8/21/75, pp. 51–52)

Hedgman said that his reason for seeking a final approval would have been to receive assurances about the practicality of the specific mode of assassination that he planned to use. (Hedgman, 8/21/75, p. 53)

All CIA officers involved in the plot to kill Lumumba testified that, by virtue of the standard operating procedure of the clandestine services, there was an implicit requirement that a field officer check back with Headquarters for approval of any major operational plan.[31] Moreover, Hedgman's cable communications with Headquarters indicate that he consistently informed Tweedy of each significant step in the formulation of assassination plans, thus allowing Headquarters the opportunity to amend or disapprove the plans. The personal cable from Dulles to the Station Officer on August 26, made it clear, however, that if Lumumba appeared as a "target of opportunity" in a situation where time did not permit referral to headquarters, Hedgeman was authorized to proceed with the assassination.

The Station Officer testified that for several months after receiving Scheider's instructions he took "exploratory steps in furtherance of the assassination plot." He sent several cables to CIA Headquarters which "probably reflected further steps I had taken," and stated that his cables to Headquarters were essentially "progress reports" on his attempts to find access to Lumumba. (Hedgman, 8/21/75, pp. 50, 59–60)

---

[31] See Tweedy, 10/9/75, I, pp. 10, 24–27; Hedgman, 8/21/75, pp. 39, 51–53; Scheider, 10/7/75, p. 92; Deputy Chief, Africa Division, affidavit, 10/17/75, p. 5.

The cable traffic conforms to the Station Officer's recollection. For two months after Scheider's arrival in the Congo, a regular stream of messages assessing prospects for the assassination operation flowed through the PROP channel between Headquarters and Leopoldville.

(ii) "Exploratory Steps"

On the basis of his talks with Scheider, Station Officer Hedgman listed a number of "possibilities" for covert action against Lumumba. At the top of the list was the suggestion that a particular agent be used in the following manner:

> HAVE HIM TAKE REFUGE WITH BIG BROTHER. WOULD THUS ACT AS INSIDE MAN TO BRUSH UP DETAILS TO RAZOR EDGE. (CIA Cable, 9/27/60)

Tweedy testified that "Big Brother" referred to Lumumba. (Tweedy, 10/9/75 II, p. 13) Tweedy and Scheider both said that this cable indicated that Hedgman's top priority plan was to instruct his agent to infiltrate Lumumba's entourage to explore means of poisoning Lumumba. (Tweedy, 10/9/75 I, p. 38, II, pp. 13–14; Scheider, 10/7/75, pp. 124–125) The Station Officer reported that he would begin to follow this course by recalling the agent to Leopoldville, and informed Headquarters:

> BELIEVE MOST RAPID ACTION CONSISTENT WITH SECURITY INDICATED * * * PLAN PROCEED ON BASIS PRIORITIES AS LISTED ABOVE, UNLESS INSTRUCTED TO CONTRARY. (CIA Cable, 9/27/60)

Scheider testified that at this point the Station Officer was reporting to Headquarters that he was proceeding to "go ahead" to carry out Scheider's instructions as quickly as possible. (Scheider, 10/7/75, pp. 121–123) Tweedy's Deputy stated that the form of the Station Officer's request would have satisfied the standard requirement for confirmation of an operational plan

> * * * it is my professional opinion that, under normal operational procedure at that time, the Station Officer would have been expected to advise Headquarters that he was preparing to implement the plan unless advised to the contrary. (Deputy Chief, Africa Division, affidavit, 10/17/75, p. 5)

On September 30, the Station Officer specifically urged Headquarters to authorize "exploratory conversations" to launch his top priority plan:

> NO REALLY AIRTIGHT OP POSSIBLE WITH ASSETS NOW AVAILABLE. MUST CHOOSE BETWEEN CANCELLING OP OR ACCEPTING CALCULATED RISKS OF VARYING DEGREES.
>
> * * * [IN] VIEW NECESSITY ACT IMMEDIATELY, IF AT ALL, URGE HQS AUTHORIZE EXPLORATORY CONVERSATIONS TO DETERMINE IF [AGENT] WILLING TAKE ROLE AS ACTIVE AGENT OR CUT-OUT THIS OP. (WOULD APPROACH ON HYPOTHETICAL BASIS AND NOT REVEAL PLANS.) IF HE APPEARS WILLING ACCEPT ROLE, WE BELIEVE IT NECESSARY REVEAL OBJECTIVE OP TO HIM.
>
> * * * REQUEST HQS REPLY [IMMEDIATELY]. (CIA Cable, Leopoldville to Tweedy, 9/30/60)

Headquarters replied:

> YOU ARE AUTHORIZED HAVE EXPLORATORY TALKS WITH [AGENT] TO ASSESS HIS ATTITUDE TOWARD POSSIBLE ACTIVE AGENT OR CUTOUT ROLE *** IT DOES APPEAR FROM HERE THAT OF POSSIBILITIES AVAILABLE [THIS AGENT] IS BEST *** WE WILL WEIGH VERY CAREFULLY YOUR INITIAL ASSESSMENT HIS ATTITUDE AS WELL AS ANY SPECIFIC APPROACHES THAT MAY EMERGE *** APPRECIATE MANNER YOUR APPROACH TO PROBLEM "HOPE *** FOR MODERATE HASTE" (CIA Cable, Deputy Chief, Africa Division to Leopoldville, 9/30/60)

Tweedy and his Deputy made it clear that the agent was being viewed as a potential assassin. (Tweedy, 10/9/75 I, p. 41; Deputy Chief, Africa Division, affidavit, 10/17/75, p. 4) Tweedy stated that it would have been proper for his Deputy to issue this cable authorizing the Station Officer to take the assassination operation "one step further" and it was "quite possible" that Richard Bissell was informed of this directive. (Tweedy, 10/9/75, pp. 42–43)

On October 7, the Station Officer reported to Headquarters on his meeting with the agent who was his best candidate for gaining access to Lumumba:

> CONDUCTED EXPLORATORY CONVERSATION WITH [AGENT] *** AFTER EXPLORING ALL POSSIBILITIES [AGENT] SUGGESTED SOLUTION RECOMMENDED BY HQS. ALTHOUGH DID NOT PICK UP BALL, BELIEVE HE PREPARED TAKE ANY ROLE NECESSARY WITHIN LIMITS SECURITY ACCOMPLISH OBJECTIVE. (CIA Cable, Station Officer to Tweedy, 10/7/60)

The Station Officer testified that the subject "explored was the agent's ability to find a means to inject the toxic material into Lumumba's food or toothpaste:

> I believe that I queried the agent who had access to Lumumba, and his entourage, in detail about just what access he actually had, as opposed to speaking to people. In other words, did he have access to the bathroom did he have access to the kitchen, things of that sort.
> I have a recollection of a having queried him on that without specifying why I wanted to know this. (Hedgman, 8/21/75, pp. 48, 60)

The Station Officer said that he was left with doubts about the wisdom or practicality of the assassination plot:

> [C]ertainly I looked on it as a pretty wild scheme professionally. I did not think that it *** was practical professionally, certainly, in a short time, if you were going to keep the U.S. out of it *** I explored it, but I doubt that I ever really expected to carry it out. (Hedgman, 8/21/75, p. 11)

(iii) The Assassination Operation Moves Forward After Scheider's Return to Headquarters: October 5–7, 1960

Despite the Station Officer's testimony about the dubious practicality of the assassination operation, the cables indicate that he planned to continue his efforts to implement the operation and sought the resources to do so successfully. For example, he urged Headquarters to send an alternate agent:

> IF HQS BELIEVE [AGENT'S CIRCUMSTANCES] BAR HIS PARTICIPATION, WISH STRESS NECESSITY PROVIDE STATION WITH QUALIFIED THIRD COUNTRY NATIONAL. (CIA Cable, Leopoldville to Tweedy, 10/7/60)

Tweedy cabled the Station Officer that he "had good discussion your colleague 7 Oct"—referring to a debriefing of Scheider upon his return to the United States. Tweedy indicated that he continued to support the assassination operation and advised (Tweedy, 10/9/75 II, pp. 48–49):

> BE ASSURED DID NOT EXPECT PROP OBJECTIVES BE REACHED IN SHORT PERIOD ∗∗∗ CONSIDERING DISPATCHING THIRD COUNTRY NATIONAL OPERATIVE WHO, WHEN HE ARRIVES, SHOULD BE ASSESSED BY YOU OVER PERIOD TO SEE WHETHER HE MIGHT PLAY ACTIVE OR CUTOUT ROLE ON FULL TIME BASIS. IF YOU CONCLUDE HE SUITABLE AND BEARING IN MIND HEAVY EXTRA LOAD THIS PLACES ON YOU, WOULD EXPECT DISPATCH [TEMPORARY DUTY] SENIOR CASE OFFICER RUN THIS OP ∗∗∗ UNDER YOUR DIRECTION. (CIA Cable, Tweedy to Station Officer, 10/7/60)[32]

According to the report of the Station Officer, Joseph Scheider left the Congo to return to Headquarters on October 5 in view of the "expiration date his material" (CIA Cable, Leopoldville to Tweedy, 10/7/60)—a reference to the date beyond which the substances would no longer have lethal strength. (Scheider, 10/7/75, pp. 132–133) The cable from the Station Officer further stated that:

> [JOE] LEFT CERTAIN ITEMS OF CONTINUING USEFULNESS. [STATION OFFICER] PLANS CONTINUE TRY IMPLEMENT OP. (CIA Cable, Leopoldville to Tweedy, 10/7/60)

Notwithstanding the influence of the Station Officer's October 7 cable that some toxic substances were left with Hedgman, Scheider specifically recalled that he had "destroyed the viability" of the biological material and disposed of it in the Congo River before he departed for the United States on October 5, 1960. (Scheider, 10/7/75, pp. 133, 117, 135–136; 10/9/75, p. 20) In the only real conflict between his testimony and Schieder's, Hedgman testified that the toxic material was not disposed of until after Lumumba was imprisoned by the Congolese in early December. (Hedgman, 8/21/75, pp. 85–86)[33]

---

[32] See Sections 5(b)–5(c), *infra,* for a detailed account of the activities in the Congo of two "third country national" agents: QJ/WIN and WI/ROGUE. See Section 5(a), *infra,* for discussion of the temporary duty assignment in the Congo of senior case officer" Michael Mulroney.

[33] Scheider said he destroyed and disposed of the toxic materials: "for the reason that it didn't look like on this trip he could mount the operational ∗∗∗ assets to do the job and ∗∗∗ the material was not refrigerated and unstable." He said that he and the Station Offices "both felt that we shouldn't go ahead with this until there were no doubts." (Scheider, 10/7/75, p. 116) The Station Officer had been unable "to find a secure enough agent with the right access" to Lumumba before the potency of the biological material was "no longer reliable." (Scheider, 10/9/75, p. 28: 10/7/75, pp. 132–133) Scheider speculated that the Station Officer's reference to retaining "items of continuing usefulness" may have meant the gloves, mask, and hypodermic syringe left with Hedgman. Scheider said: "perhaps he is talking about leaving these accessory materials in case there will be a round two of this, and someone brings more material." (Scheider, 10/7/75, p. 135)

The central point remains that the Station Officer planned to continue the assassination effort, by whatever means, even after Scheider's departure. (Scheider, 10/7/75, p. 143) Scheider was under the impression that the Station Officer was still authorized to move ahead with an assassination attempt against Lumumba at that point, although he would have continued to submit his plans to Headquarters. (Scheider, 10/7/75, p.135; 10/9/75, pp. 20–21)[34]

(iv) Headquarters Continues to Place "Highest Priority" on the Assassination Operation

SUMMARY

The cable traffic during this period demonstrates that there was a clear intent at Headquarters to authorize and support rapid progress of the assassination operation. Even after Lumumba placed himself in the protective custody of the United Nations, CIA Headquarters continued to regard his assassination as the "highest priority" of covert action in the Congo. The cables also show an intent at Headquarters to severely restrict knowledge of the assassination operation among officers in CIA's Africa Division and among United States diplomatic personnel in the Congo, excluding, even those who were aware of, and involved in, other covert activities.

The Station Officer, despite the burden of his other operational responsibilities, was actively exploring, evaluating, and reporting on the means and agents that might be used in an attempt to assassinate Lumumba. When his implementation of the assassination operation was thwarted by the failure of his prime candidate to gain access to Lumumba, Hedgman requested additional operational and supervisory personnel to help him carry out the assignment, which he apparently pursued until Lumumba was imprisoned by Congolese authorities.

On October 15, 1960, shortly after Tweedy offered additional manpower for the assassination operation, a significant pair of cables were sent from CIA Headquarters to Leopoldville.

One cable was issued by a desk officer in CIA's Africa Division, released under Bronson Tweedy's signature, and transmitted through standard CIA channels, thus permitting distribution of the message to appropriate personnel in the CIA Station and the

---

In support of his position the Station Officer speculated that it was "possible" that be had preserved the poisons in his safe until after Lumumba's death. (Hedgman, 8/21/75, p. 85) He said that after Scheider's visit, he locked the toxic material in the bottom drawer of his safe, "probably" sealed in an envelope marked "Eyes Only" with his name on it. (Hedgman, 8/21/75, pp. 48–49) He did not recall taking the materials out of his safe except when he disposed of them months later. (Hedgman, 8/21/75, p. 84)

Both Scheider and the Station Officer specifically recalled disposing of the toxic material in the Congo River and each recalled performing the act alone. (Scheider, 10/7/75, pp. 117–118; Hedgman, 8/21/75, p. 84)

The Station Officer's testimony is bolstered by Michael Malroney's account that when he arrived in the Congo nearly a month after Scheider had returned to Headquarters. Hedgman informed him that there was a lethal virus in the station safe. (See Section 5(a) (iii), *infra*.) Moreover, the Station Officer distinctly remembered disposing of the medical paraphernalia. (Hedgman, 8/21/75, p. 84) This would indicate that, at the least, the operation had not been "stood down" to the point of disposing of all traces of the plot until long after Scheider's departure from the Congo.

[34] For Tweedy's testimony about the operational authority possessed by the Station Officer on October 7, see Section 4(h), *infra.*

United States Embassy. (Tweedy, 10/9/75 I, pp. 60–62) The cable discussed the possibility of covertly supplying certain Congolese leaders with funds and military aid and advised:

> ONLY DIRECT ACTION WE CAN NOW STAND BEHIND IS TO SUPPORT IMMOBILIZING OR ARRESTING [LUMUMBA], DESIRABLE AS MORE DEFINITIVE ACTION MIGHT BE. ANY ACTION TAKEN WOULD HAVE TO BE ENTIRELY CONGOLESE. (CIA Cable, Director to Leopoldville, 10/15/60)

On the same day Tweedy dispatched, a second cable, via the PROP channel for Hedgman's "Eyes Only," which prevented the message from being distributed to anyone else, including the Ambassador.[35] Tweedy's Deputy stated that "the cable which carried the PROP indicator would have controlling authority as between the two cables." (Deputy Chief, Africa Division affidavit, 10/17/75, p. 4) The second cable stated:

> YOU WILL NOTE FROM CABLE THROUGH NORMAL CHANNEL CURRENTLY BEING TRANSMITTED A PARA[GRAPH] ON PROP TYPE SUGGESTIONS. YOU WILL PROBABLY RECEIVE MORE ALONG THESE LINES AS STUMBLING BLOC [LUMUMBA] REPRESENTS INCREASINGLY APPARENT ALL STUDYING CONGO SITUATION CLOSELY AND HIS DISPOSITION SPONTANEOUSLY BECOMES NUMBER ONE CONSIDERATION.
>
> RAISE ABOVE SO YOU NOT CONFUSED BY ANY APPARENT DUPLICATION. THIS CHANNEL REMAINS FOR SPECIFIC PURPOSE YOU DISCUSSED WITH COLLEAGUE AND ALSO REMAINS HIGHEST PRIORITY. (CIA Cable, Tweedy to Station Officer, 10/15/60)

Tweedy testified that the "specific purpose discussed with colleague" referred to the Station Officer's discussion of "assassination with Scheider." He stated that the premise of his message was that "there is no solution to the Congo as long as Lumumba stays in a position of power or influence there." (Tweedy, 10/9/75 I, pp. 59, 60)[36]

Tweedy went on to request the Station Officer's reaction to the prospect of sending a senior CIA case officer to the Congo on a "direct assignment ∗ ∗ ∗ to concentrate entirely this aspect" (CIA Cable, Tweedy to Station Officer, 10/15/60).[37]

The cable also provided an insight into why the assassination operation had not progressed more rapidly under the Station Officer:

> SEEMS TO US YOUR OTHER COMMITMENTS TOO HEAVY GIVE NECESSARY CONCENTRATION PROP.

---

[35] Hedgman testified that he did not discuss the assassination operation with anyone at the United States embassy in Leopoldville. Moreover, he testified that he never discussed the prospect of assassinating Lumumba with Clare H. T. Timberlake, who was the Ambassador to the Congo at that time. (Hedgman, 8/21/75, p. 91)

[36] See Section 4(h), *infra,* for Tweedy's testimony on the conditions under which he believed the operation was authorized to proceed.

This referred to CIA officer Michael Mulroney (Tweedy, 10/9/75 I, p. 56), who testified that in late October he was asked by Richard Bissell to undertake the mission of assassinating Lumumba.

[37] For a full account of the meeting between Bissell and Mulroney and Mulroney's subsequent activities in the Congo, see Section 5 (a), *infra.*

In contradiction of the limitations on anti-Lumumba activity outlined in the cable sent through normal channels, Tweedy's cable suggested:

> POSSIBILITY USE COMMANDO TYPE GROUP FOR ABDUCTION [LUMUMBA], EITHER VIA ASSAULT ON HOUSE UP CLIFF FROM RIVER OR, MORE PROBABLY, IF [LUMUMBA] ATTEMPTS ANOTHER BREAKOUT INTO TOWN * * * REQUEST YOUR VIEWS. (CIA Cable, Tweedy to Station Officer, 10/15/60)

Two days later the Station Officer made a number of points in a reply to Tweedy. First, the agent he had picked for the assassination operation had difficulty infiltrating Lumumba's inner circle:[38]

> HAS NOT BEEN ABLE PENETRATE-ENTOURAGE. THUS HE HAS NOT BEEN ABLE PROVIDE OPS INTEL NEEDED THIS JOB. * * * ALTHOUGH MAINTAINING PRIORITY INTEREST THIS OP, ABLE DEVOTE ONLY LIMITED AMOUNT TIME, VIEW MULTIPLE OPS COMMITMENTS. * * * BELIEVE EARLY ASSIGNMENT SENIOR CASE OFFICER HANDLE PROP OPS EXCELLENT IDEA * * * IF CASE OFFICER AVAILABLE [STATION OFFICER] WOULD DEVOTE AS MUCH TIME AS POSSIBLE TO ASSISTING AND DIRECTING HIS EFFORTS, (CIA Cable, 10/17/60)

The Station Officer concluded this cable with the following cryptic recommendation, reminiscent of his testimony that he may have "suggested" shooting Lumumba to Scheider as an alternative to poisoning (Hedgman, 8/21/75, pp. 27–29):

> IF CASE OFFICER SENT, RECOMMEND HQS POUCH SOONEST HIGH POWERED FOREIGN MAKE RIFLE WITH TELESCOPIC SCOPE AND SILENCER. HUNTING GOOD HERE WHEN LIGHTS RIGHT. HOWEVER AS HUNTING RIFLES NOW FORBIDDEN, WOULD KEEP RIFLE IN OFFICE PENDING OPENING OF HUNTING SEASON. (CIA Cable, 10/17/60)

Tweedy testified that the Station Officer's recommendation clearly referred to sending to the Congo via diplomatic pouch a weapon suited for assassinating Lumumba. (Tweedy, 10/9/75 I, p. 64) Senior case officer Mulroney stated that lie never heard discussion at Headquarters of sending a sniper-type weapon to the Congo, nor did he have any knowledge that such a weapon had been "pouched" to the Congo. (Mulroney affidavit, 11/7/75)

The oblique suggestion of shooting Lumumba at the "opening of hunting season" could be interpreted as a plan to assassinate Lumumba as soon as lie was seen outside the residence where he remained in U.N. protective custody. Tweedy interpreted the cable to mean that "an operational plan involving a rifle" had not yet been formulated by the Station Officer and that the "opening of hunting season" would depend upon approval of such a plan by CIA headquarters. (Tweedy, 10/9/75 1, pp. 64–65)

A report sent the next month by the Station Officer through the PROP channel for Tweedy's "Eyes Alone" indicated that, whatever the intention about moving forward with a plan for assassination by rifle fire, Lumumba was being viewed as a "target" and his movements were under close surveillance. Hedgman's cable described the stalemate which prevailed from mid-September until Lumumba's departure for Stanleyville on November 27; Lumumba was virtually a prisoner in U.N. custody, and inaccessible to CIA agents and the Congolese:

---

[38] This agent left Leopoldville "sometime in October" and their discussions terminated. (Hedgman, 8/21/75, p. 61)

TARGET HAS NOT LEFT BUILDING IN SEVERAL WEEKS. HOUSE GUARDED DAY AND NIGHT BY CONGOLESE AND UN TROOPS ***. CONGOLESE TROOPS ARE THERE TO PREVENT TARGET'S ESCAPE AND TO ARREST HIM IF HE ATTEMPTS. UN TROOPS THERE TO PREVENT STORMING OF PALACE BY CONGOLESE. CONCENTRIC RINGS OF DEFENSE MAKE ESTABLISHMENT OF OBSERVATION POST IMPOSSIBLE. ATTEMPTING GET COVERAGE OF ANY MOVEMENT INTO OR OUT OF HOUSE BY CONGOLESE ***. TARGET HAS DISMISSED MOST OF SERVANTS SO ENTRY THIS MEANS SEEMS REMOTE. (CIA Cable, Station Officer to Tweedy, 11/14/60)

(h) Tweedy/Bissell Testimony: Extent of Implementation; Extent o f Authorization

SUMMARY

The testimony of Richard Bissell and Bronson Tweedy is at some variance from the picture of the assassination plot presented by the Station Officer and by the cable traffic from the period.

The cables demonstrate that CIA Headquarters placed the "highest priority" on the effort to assassinate Lumumba. They also show that the assassination operation involving Scheider and the Station Officer was initiated by a cable signed personally by Bissell and Tweedy and transmitted in a specially restricted cable channel established solely for communications about this operation. Bissell and Tweedy both testified to an absence of independent recollection of Scheider's assignment in the Congo and of any specific operation to poison Lumumba.

The cables appear to indicate that the Station Officer was authorized to proceed with an assassination attempt if he determined it to be a feasible, secure operation and if time did not permit referral to Headquarters for approval. Tweedy alone testified that the Station Officer was empowered only to explore and assess the means of assassinating Lumumba and not to proceed with an assassination attempt even when "time did not permit" referral to Headquarters.

(i) Tweedy's Testimony About the Scope of the Assassination Operation

As Chief of the Africa Division, Bronson Tweedy had the principal supervisory responsibility at CIA Headquarters for the operations of the Station Officer Hedgman in Leopoldville. Most of the reports and recommendations cabled by Hedgman on the assassination operation were marked for Tweedy's "Eyes Only." Through Tweedy, instructions were issued, plans were approved, and progress reports were assessed concerning the effort to assassinate Lumumba.[39]

[39] Tweedy personally signed both the cable which initially informed the Station Officer that "JOE" would arrive in Leopoldville with an assignment (CIA Cable, Bissell, Tweedy to Station Officer, 9/19/60) and the cable of October 7 indicating that he had debriefed Scheider upon his return from the Congo. (CIA Cable, Tweedy to Station Officer, 10/7/60) Tweedy was also the "Eyes Only" recipient of Hedgman's reports on Scheider's arrival in the Congo (CIA Cable, Station Officer to Tweedy, 9/27/60) and of subsequent communications about the top priority plan that emerged from the discussions between Scheider and Hedgman: i.e., infiltrating an agent into Lumumba's entourage to administer a lethal poison to the Congolese leader, (CIA Cable, Station Officer to Tweedy, 9/30/60; CIA Cable, Station Officer to Tweedy, 10/7/60; CIA Cable, Station Officer to Tweedy, 10/17/60) See Sections 4(a)–4(e) *supra* for a full treatment of the cables sent in the PROP channel between Tweedy and the Station Officer in Leopoldville.

Before reviewing all of the cables, Tweedy testified that he had no knowledge of the plot to poison Lumumba. (Tweedy, 9/9/75, pp. 30–31) He stated that if Scheider went to the Congo as a courier carrying lethal biological material, "I will bet I knew it, but I don't recall it." (Tweedy, 9/9/75, p. 35)

Tweedy commented that rather than questioning the truth of the Station Officer's testimony,[40] the discrepancies between their testimony could be attributed to his own lack of recall.[41]

Even after he reviewed the cables on the PROP operation, Tweedy said that he did not recall talking to Scheider about an assignment to the Congo, although he assumed he had done so. Tweedy's review enabled him to "recall the circumstances in which these things occurred; and there's no question that Mr. Scheider went to the Congo." (Tweedy, 10/9/75 I, p. 13; II, pp. 5–6)[42]

Despite Tweedy's lack of recollection about the actual plot to poison Lumumba, he recalled discussing the feasibility of an assassination attempt against Lumumba with Bissell and communicating with the Station Officer about gaining access to Lumumba for this purpose. (Tweedy, 9/9/75, pp. 14–15, 19–21)

Tweedy characterized his discussions with Bissell about assassinating Lumumba as "contingency planning" (Tweedy, 9/9/75, p. 28):

TWEEDY. ∗∗∗ I think it came up in the sense that Dick would have said we probably better be thinking about whether it might ever be necessary or desirable to get rid of Lumumba, in which case we presumably should be in position to assess whether we could do it or not successfully.

Q. Do it, meaning carry off an assassination?

TWEEDY. Yes, but it was never discussed with him in any other sense but a planning exercise. ∗∗∗ never were we instructed to do anything of this kind. We were instructed to ask whether such a thing would be feasible and to have the Station Officer thinking along those lines as well. (Tweedy, 9/9/75, pp. 15, 28)

Tweedy testified that Bissell never authorized him to proceed beyond the planning stage to move forward with an assassination attempt. (Tweedy, 10/9/75 I, p. 17)

Tweedy characterized the entire assassination operation as "exploratory":

> This involved the launching of the idea with the field so they could make the proper operational explorations into the feasibility of this, reporting back to Headquarters for guidance. At no point

[40] Tweedy expressed a high regard for the credibility of the Station Officer. Tweedy said that he never had occasion to doubt Hedgman's veracity or integrity, adding, "I would trust his memory and I certainly trust his integrity." (Tweedy, 9/9/75, p. 36)

[41] Tweedy explained his difficulty in recalling the assassination operation:

"[T]he things that I recall the most vividly about all my African experiences were ∗∗∗ the things I was basically concerned with all the time, which was putting this Division together and the rest of it. When it comes to operational detail I start getting fuzzy and you would have thought with something like thinking about Mr. Lumumba in these terms that I would have gone to bed and got up thinking about Lumumba, I can assure you this wasn't the case." (Tweedy, 9/9/75, p 34)

[42] For a detailed treatment of Tweedy's testimony on Scheider's assignment to the Congo and the assassination operation against Lumumba, see Sections 4(a)–(g), *supra.*

> was the field given carte blanche if they thought they had found a way to do the job, just to carry it out with no further reference. (Tweedy, 10/9/75 II, p. 22)

He testified that the period of exploration of access to Lumumba remained "a planning interval and at no point can I recall that I ever felt it was imminent that somebody would say 'go.' " (Tweedy, 9/9/75, pp. 18–19)

Tweedy stated that, despite his inability to specifically recall his directive to Scheider, he would not have given the Station Officer an instruction "to use this [toxic] material and go ahead and assassinate Lumumba, as if * * * that is all the authority that was necessary." He said that:

> Under no circumstances would that instruction have been given by me without reference to higher authority up through the chain of command * * * my higher authority, in the first instance, would be Mr. Bissell * * * and I know Mr. Bissell would have talked to Mr Dulles. (Tweedy, 10/9/75 I, pp. 17–18; 10/9/75 II, pp. 25, 33)

It is difficult to reconcile some of the cables and the testimony of Scheider and Hedgman with Tweedy's testimony that there was "no misunderstanding" that the PROP operation was purely exploratory "contingency planning" and that no authorization was granted for attempting an assassination without checking back with headquarters.

For example, Dulles' August 26 directive appeared to indicate wide latitude for making operational decisions in the field "where time does not permit referral" to Headquarters.

Tweedy testified that sending a potentially lethal biological material with a short period of toxicity to the Congo did not mean that the Station Officer was empowered to take action without seeking final approval from Headquarters.

> TWEEDY: If, as a result of the Station focusing on the problem for the first time, as a result of Headquarters' request, they had come up with a plan that they thought was exceedingly solid and which Headquarters approved, it is not surprising, perhaps, that we wanted the materials there to take advantage of such * * * an unlikely event.
>
> Q: Because Scheider took lethal materials to the Congo with him that had such a short period of lethality, were you not contemplating at that tine that the operation might well move from the exploration phase to the implementation phase just as soon as Scheider and Hedgman determined that it was feasible?
>
> TWEEDY: I think I would put it quite differently. I think that I would say that we would have been remiss in not being in a position to exploit, if we reached the point where we all agreed that the thing was possible. (Tweedy, 10/9/75 I, pp. 49–50)

The dispatch of toxic material and medical paraphernalia to the Congo certainly demonstrates that the "exploration" of the feasibility of assassinating Lumumba had progressed beyond mere assessment and "contingency planning."

Tweedy further disagreed that the Station Officer's October 7 message that he would "continue try implement op[eration]" signified that the Officer was prepared to proceed to "implement" an assassination attempt:

> He would continue to explore the possibilities of this operation and continue to report to Headquarters. That is all this means. It does not mean that * * * he would try to pull off the

> operation without further reference to Headquarters * * * [H]e was to continue to explore it to determine whether or not there was a feasible means. (Tweedy, 10/9/75 II, pp. 14–15)

Finally, Tweedy's recollection that a "go ahead" on the assassination operation was never imminent is brought into question by the cable he sent for Hedgman's "Eyes Only" on October 15 to assure him that there was a policy-level consensus that Lumumba's "disposition spontaneously becomes number one consideration" and that the PROP operation "remains highest priority." (CIA Cable, Tweedy to Station, 10/15/60)

(ii) Bissell's Testimony About Moving the Assassination Operation From Planning to Implementation

Richard Bissell testified that he did not remember discussing the feasibility of assassinating Lumumba with Bronson Tweedy, but it seemed "entirely probable" to him that such discussions took place. Bissell, who did not review the cable traffic, said he "may have" given Tweedy specific instructions about steps to further an assassination plan, but he did not remember doing so. He said that seeking information from the Station Officer about access for poisoning or assassinating Lumumba by other means would "almost certainly" have been a "major part" of his "planning and preparatory activity" but he had no specific recollection of cable communications on this subject. He did recall that the Station Officer had an agent who supposedly had direct access to Lumumba. (Bissell, 9/10/75, pp. 3, 4, 6–8, 80)

Bissell testified that he "most certainly" approved any cables that Tweedy sent to the Station Officer seeking information about gaining access to Lumumba because in "a matter of this sensitivity," Tweedy probably would have referred cables to him for final dispatch. But Bissell added:

> I think Mr. Tweedy, on the basis of an oral authorization from me, would have had the authority to send such a cable without my signing off on it. (Bissell, 9/10/75, p. 8)

Bissell's failure to recall discussing his assignment to Michael Mulroney[43] with Tweedy provided a basis for his speculation that Tweedy might also have been unaware of the true purpose of Scheider's visit. (Bissell, 9/10/75, pp. 20–22)

Bissell did not recall cables concerning Scheider's mission, and confirming that Scheider's instructions were to be followed; but he said "this sounds highly likely * * * I would expect, given the background, that the confirmation would have been forthcoming." (Bissell, 9/10/75, p. 43)

Bissell said that it was "very probable" that he discussed the assassination of Lumumba with Scheider, who was then his science advisor. On a number of occasions he and Scheider had discussed "the availability of means of incapacitation, including assassination." Although he had no "specific recollection," Bissell assumed that, if Scheider went to the Congo, Bissell would have approved the mission, which "might very well" have dealt with the assassination of Lumumba. (Bissell, 9/10/75, pp. 14, 60, 18, 20, 44)

Bissell testified that it would not have been against CIA policy in the fall of 1960 to send poisons to the Congo. He characterized "the act of taking the kit to the Congo * * * as still in the planning stage." (Bissell, 9/10/75, pp. 35, 49). He acknowledged, however, that:

---

[43] Bissell's assignment to Mulroney is discussed in Sections 5(a) (i) and 5(a) (ii), *infra*.

> It would indeed have been rather unusual to send such materials—a specific kit * * * of this sort—out to a relatively small Station, unless planning for their use was quite far along. (Bissell, 9/10/7, p. 37)

Nonetheless, Bissell said that he "probably believed" that he had sufficient authority at that point to direct CIA officers to move from the stage of planning to implementation. (Bissell, 9/10/75, pp. 60–61) Although he did not have a specific recollection, Bissell assumed that if Scheider had instructed Hedgman to assassinate Lumumba, Scheider would not have been acting beyond the mandate given to him by Bissell and the assassination plot would then have "passed into an implementation phase." (Bissell, 9/10/75, pp. 39, 41, 49)

5. The Question of a Connection Between the Assassination Plot and Other Actions of CIA Officers and Their Agents in the Congo

SUMMARY

Michael Mulroney, a senior CIA officer in the Directorate for Plans, testified that in October 1960 he had been asked by Richard Bissell to go to the Congo to carry out the assassination of Lumumba. Mulroney said he refused to participate in an assassination operation, but proceeded to the Congo to attempt to draw Lumumba away from the protective custody of the U.N. guard and place him in the hands of Congolese authorities. (Mulroney, 6/9/75, pp. 11–14)

Shortly after Mulroney's arrival in the Congo, he was joined by QJ/WIN, a CIA agent with a criminal background.[44] Late in 1960, WI/ROGUE, one of Hedgman's operatives approached QJ/WIN with a proposition to join an "execution squad." (CIA Cable, Leopoldville to Director, 12/7/60)

It is unlikely that Mulroney was actually involved in implementing the assassination assignment. Whether there was any connection between the assassination plot and either of the two operatives—QJ/WIN and WI/ROGUE—is less clear.

(a) Mulroney's Assignment in the Congo

(i) Mulroney's Testimony That He Went to the Congo After Refusing an Assassination Assignment From Bissell

In early October, 1960, several PROP cables discussed a plan to send a "senior case officer" to the Congo to aid the overburdened Station Officer with the assassination operation.[45] Shortly after the Station Officer's request on October 17, for a senior case officer to concentrate on the assassination operation. Bissell broached the subject with Mulroney. At the time, Mulroney was the Deputy Chief of an extraordinarily secret unit within the Directorate of Plans. (Mulroney, 6/9/75, p. 8)

Mulroney testified that in October of 1960, Bissell asked him to undertake the mission of assassinating Patrice Lumumba:

> MULRONEY: He called me in and told me he wanted to go down to the Belgian Congo, the former Belgian Congo, and to eliminate Lumumba * * *.

---

[44] See Part III, Section c, of this Report for a discussion of the CIA's use of QJ/WIN in developing a stand-by assassination capability in the Executive Action project.

[45] See Section 4(g), *supra*, for full treatment of these cables.

Q: What did you understand him to mean by eliminate?

MULRONEY: To kill him and thereby eliminate his influence.

Q: What was the basis for your interpreting his remarks, whatever his precise language, as meaning that he was talking about assassination rather than merely neutralizing him through some other means?

MULRONEY: It was not neutralization ∗∗∗ clearly the context of our talk was to kill him. (Mulroney, 6/9/75, pp. 11–12, 19, 43)

Mulroney testified:

> I told him that I would absolutely not have any part of killing Lumumba. He said, I want you to go over and talk to Joseph Scheider. (Mulroney, 6/9/75, p. 12)

Mulroney said that it was "inconceivable that Bissell would direct such a mission without the personal permission of Allen Dulles":

> I assumed that he had authority from Mr. Dulles in such as important issue, but it was not discussed [with me], nor did he purport to have higher authority to do it. (Mulroney, 9/9/75, pp. 15, 44)

Mulroney then met promptly with Scheider and testified that he was "sure that Mr. Bissell had called Scheider and told him I was coming over" to his office. Scheider told Mulroney "that there were four or five ∗∗∗ lethal means of disposing of Lumumba ∗∗∗. One of the methods was a virus and the others included poison." Mulroney said that Scheider "didn't even hint ∗∗∗ that he had been in the Congo and that he had transported any lethal agent to the Congo." (Mulroney, 6/9/75, pp. 12–13; 9/11/75, pp. 7–7A)

Mulroney testified that after speaking with Scheider:

> I then left his office, and I went back to Mr. Bissell's office, and I told him in no way would I have any part in the assassination of Lumumba ∗∗∗ and reasserted in absolute terms that I would not be involved in a murder attempt. (Mulroney, 9/11/75, p. 43)[46]

---

[46] When asked at the conclusion of his testimony to add anything to the record that he felt was necessary to present a full picture of the operation against Lumumba, Mulroney volunteered a statement about the moral climate in which it took place:

"All the people that I knew acted in good faith. I think they acted in the light of ∗∗∗ maybe not their consciences, but in the light of their concept of patriotism. [T]hey felt that this was in the best interests of the U.S. I think that we have to much of the 'good German' in us, in that we do something because the boss says it is okay. And they are not essentially evil people. But you can do an awful lot of wrong in this.

"∗∗∗ This is such a dishonest business that only honest people can be in it. That is the only thing that will save the Agency and make you trust the integrity of what they report ∗∗∗. An intelligence officer ∗∗∗ must be scrupulous and he must be moral ∗∗∗ he must have personal integrity ∗∗∗. They must be particularly conscious of the moral element in intelligence operations." (Mulroney, 9/11/75, pp. 57, 61)

Earlier in his testimony, Mulroney succinctly summarized his philosophical opposition to assassinating Lumumba: "murder corrupts." (Mulroney, 9/11/75, p. 9)

Mulroney said that in one of his two conversations with Bissell about Lumumba, he raised the prospect "that conspiracy to commit murder being done in the District of Columbia might be in violation of federal law." He said that Bissell "airily dismissed" this prospect. (Mulroney, 6/9/75, p. 14)

Although he refused to participate in assassination, Mulroney agreed to go to the Congo on a general mission to "neutralize" Lumumba "as a political factor" (Mulroney, 9/11/75, pp. 43–44):

> I said I would go down and I would have no compunction about operating to draw Lumumba out [of UN custody], to run an operation to neutralize his operations which were against Western interests, against, I thought, American interests. (Mulroney, 6/9/75, p. 13)[47]

Although Mulroney did not formulate a precise plan until he reached the Congo, he discussed a general strategy with Bissell:

MULRONEY: I told Mr. Bissell that I would be willing to go down to neutralize his activities and operations and try to bring him out [of UN custody] and turn him over to the Congolese authorities.

Senator MONDALE: Was it discussed then that his life might be taken by the Congolese authorities?

MULRONEY: It was, I think, considered * * * not to have him killed, but then it would have been a Congolese being judged by Congolese for Congolese crimes. Yes, I think it was discussed. (Mulroney, 6/9/75, p. 38)

According to Mulroney there was a "very, very high probability" that Lumumba would receive capital punishment at the hands of the Congolese authorities. But he "had no compunction about bringing him out and then having him tried by a jury of his peers." (Mulroney, 6/9/75, pp. 24, 14)

Despite Mulroney's expressed aversion to assassination and his agreement to undertake a more general mission to "neutralize" Lumumba's influence, Bissell continued pressing him to consider an assassination operation:

> In leaving at the conclusion of our second discussion * * * he said, well, I wouldn't rule out that possibility—meaning the possibility of the elimination or the killing of Lumumba * * *. In other words, even though you have said this, don't rule it out * * *. There is no question about it, he said, I wouldn't rule this other out, meaning the elimination or the assassination. (Mulroney, 9/11/75, p. 45)

Mulroney distinctly recalled that after his second discussion with Bissell, he meet with Richard Helms, who was then Deputy to the DDP and Chief of Operations in the clandestine services division, in order to make his opposition to assassinating Lumumba a matter of record (Mulroney, 9/11/75, pp. 44–45):

---

[47] Bissell also recalled that, after discussing assassination with Mulroney, Mulroney went to the Congo "with the assignment * * * of looking at other ways of neutralizing Lumumba." (Bissell, 9/10/75, p. 53)

> [I]n the Agency, since you don't have documents, you have to be awfully canny and you have to get things on record, and I went into Mr. Helms' office, and I said, Dick, here is what Mr. Bissell proposed to me, and I told him that I would under no conditions do it, and Helms said, 'you're absolutely right.' (Mulroney 6/9/75, pp. 15–16)

Helms testified that it was "likely" that he had such a conversation with Mulroney and he assumed that Mulroney's version of their conversation was correct. (Helms, 9/16/75, pp. 22–23)[48]

William Harvey was Mulroney's immediate superior at that time[49] He testified:

> Mr. Mulroney came to me and said that he had been approached by Richard Bissell ∗∗∗ to undertake an operation in the Congo, one of the objectives of which was the elimination of Patrice Lumumba. He also told me that he had declined to undertake this assignment. (Harvey, 6/25/75, p. 9)

Harvey said that in a later conversation with Bissell, Bissell told him that he had asked Mulroney to undertake such an operation. (Harvey, 6/25/75, p. 9)

Tweedy's Deputy, who aided in making preparations for Mulroney's trip to the Congo, recalled that Mulroney had "reacted negatively" to Bissell's request to undertake an assassination operation. (Deputy Chief, Africa Division affidavit, 10/17/75, p. 2) He stated:

> Despite the fact that Mulroney had expressed a negative reaction to this assignment, it was clear to me that when Mulroney went to the Congo, exploration of the feasibility of assassinating Lumumba was part of his assignment from Bissell. As far as I know, Mulroney was not under assignment to attempt to assassinate Lumumba, but rather merely to make plans for such an operation. (Deputy Chief, Africa Division affidavit, 10/17/75, p. 2)

In Tweedy's mind, Mulroney's eventual mission to the Congo was also linked to assessing the possibility for assassinating Lumumba rather than to a general plan to draw Lumumba out of U.N. custody. (Tweedy, 9/9/75, pp. 24, 26)

Mulroney testified, however, that because he was "morally opposed to assassination" he would "absolutely not" have explored the means by which such access could be gained, nor would he have undertaken a mission to the Congo to assess an assassination operation even if it were directed by someone else. (Mulroney, 9/11/75, p. 26)

Mulroney said that he departed for the Congo within forty-eight hours of his second discussion with Bissell. (Mulroney, 9/11/75, pp. 45–46)

(ii) Bissell's Testimony About the Assignment to Mulroney

Bissell remembered "very clearly" that he and Mulroney discussed the assassination of Lumumba in the fall of 1960 (Bissell, 6/9/75, pp. 74–750 and the Mulroney reacted negatively. (Bissell 9/11/75, p. 18) Accrodingly to Bissell, Mulroney said that assassination

---

[48] Helms testified that he did not inquire further into the subject of this conversation in any way. He did not recall why Mulroney had gone to the Congo or what his mission was. (Helms, 9/16/75, pp. 32–33)

[49] Harvey was later centrally involved in the Castro case and the Executive Action project. See Parts III (B) and Part III (C), *infra*.

"was an inappropriate action and that the desired object could be accomplished better in other ways." (Bissell, 6/11/75, p. 54)

Bissell's testimony differs from Mulroney's account on only one important point—the degree to which Bissell's initial assignment to Mulroney contemplated the mounting of an operation as opposed to contingency planning. Mulroney flatly testified that Bissell requested him to attempt to kill Lumumba. In his first testimony on the subject, Bissell said that he asked Mulroney "to investigate the possibility of killing Lumumba." (Bissell, 6/11/75, p. 54; *see also* pp. 55, 75) In a later appearance, however, Bissell stated that Mulroney "had been asked to plan and prepare for" the assassination of Lumumba. (Bissell, 9/10/75, p. 24)

Bissell said that after his conversations with Mulroney, he considered "postponing" the assassination operation:

> I seem to recollect that after this conversation with him, I wanted this put very much on the back burner and inactivated for quite some time. Now that doesn't rule out the possibility that some action through completely different channels might have gone forward. But the best of my recollection is, I viewed this not only as terminating the assignment for him, but also as reason for at least postponing anything further along that line. (Bissell, 9/10/75, pp. 25–26)

(iii) Mulroney Informed of Virus in Station Safe Upon Arriving in Congo: November 3, 1960

On October 29, the Station Officer was informed that Michael Mulroney would soon arrive in Leopoldville "in furtherance this project." (CIA Cable Deputy Chief, Africa Division, to Station Officer 10/29/60) On November 3, Mulroney arrived in Leopoldville. (CIA Cable, Leopoldville to Director, 11/4/60) Hedgman said it was "very possible" that he regarded the dispatch to the Congo of a senior officer as a signal that CIA Headquarters was "dissatisfied with my handling" of Scheider's instructions. (Hedgman, 8/21/75, p. 42)

Hedgman had only a general picture of Mulroney's assignment:

> I understood it to be that—similar to mine, that is, the removal or neutralization of Lumumba * * * I have no clear recollection of his discussing the assassination. (Hedgman, 8/21/75, p. 54)

Station Officer Hedgman said that he did not recall if Mulroney indicated whether he was considering assassination as a means of "neutralizing" Lumumba. Hedgman said, "in view of my instructions, I may have assumed that he was" considering assassination. Generally, however, the Station Officer perceived Mulroney as unenthusiastic about his assignment. (Hedgman, 8/21/75, pp. 55, 56, 88–89)

When Mulroney arrived in the Congo, he met with the Station Officer, who informed him that there was "a virus in the safe." (Mulroney, 9/11/75, p. 7–A; 6/9/75, p. 16) Mulroney said he assumed it was a "lethal agent," although the Station Officer was not explicit:

> I knew it wasn't for somebody to get his polio shot up to date. (Mulroney, 6/9/75, pp. 16, 37)[50]

[50] Mulroney added that if the virus was to be used for medical purposes, "It would have been in the custody of the State Department" personnel, not the CIA Station. (Mulroney, 6/9/75, p. 36)

Mulroney said that he did not recall the Station Officer's mentioning the source of the virus, but:

> It would have had to come from Washington, in my estimation, and I would think, since it had been discussed with Scheider that it probably would have emanated from his office. (Mulroney, 6/9/75, p. 28)[51]

Hedgman did not recall discussing Scheider's trip to the Congo with Mulroney, but "assumed" that he did so. (Hedgman, 8/21/75, pp. 60–61)

Mulroney was "certain" that the virus had arrived before he did. (Mulroney, 6/9/75, p. 24) He was surprised to learn that such a virus was at the Leopoldville Station because he had refused an assassination mission before departing for the Congo. (Mulroney, 6/9/75, p. 17)

Mulroney stated that he knew of no other instance where a CIA Station had possessed lethal biological substances. He assumed that its purpose was assassination, probably targeted against Lumumba. (Mulroney, 9/11/75, p. 50):

> My feeling definitely is that it was for a specific purpose, and was just not an all-purpose capability there, being held for targets of opportunity, unspecified targets. (Mulroney, 9/11/75, p. 49)

Mulroney said that the Station Officer never indicated that Mulroney was to employ the virus, that he "never discussed his assassination effort, he never even indicated that this was one." (Mulroney, 9/11/75, pp. 52, 54)

While Station Officer Hedgman had no direct recollection of discussing the assassination operation with Mulroney, he "assumed" that he had at least mentioned the problem of gaining access to Lumumba for the purpose of assassinating him. (Hedgman, 8/21/75, pp. 55, 60)

Mulroney was "sure" that he "related everything" to Hedgman about his conversations with Bissell concerning the assassination of Lumumba. (Mulroney, 9/11/75, p. 46) Hedgman, however, did not recall learning this from Mulroney. (Hedgman, 8/21/75, p. 56)

Mulroney said that his discussions of assassination with Hedgman were general and philosophical, dealing with "the morality of assassinations. (Mulroney, 9/11/75, pp. 46, 54):

> From my point of view I told him I had moral objections to it, not just qualms, but objections. I didn't think it was the right thing to do. (Mulroney, 9/11/75, p. 9)

When asked to characterize Hedgman's attitude toward assassination based on those discussions, Mulroney said:

> He would not have been opposed in principle to assassination in the interests of national security * * *. I know that he is a man of great moral perception and decency and honor * * *. And

[51] When Mulroney was informed about Hedgman's testimony concerning Scheider's trip to the Congo and the plot to poison Lumumba, he said, "I believe absolutely in its credibility. Mulroney found nothing in the facts as he knew them, nor in Hedgman's character, to raise a question about that testimony. He regarded Hedgman as "an honest and a decent man—a totally truthful man." (Mulroney, 9/11/75, pp. 19, 53, 56)

> that it would disturb him to be engaged in something like that. But I think I would have to say that in our conversations, my memory of those, at no time would he rule it out as being a possibility. (Mulroney, 9/11/75, p. 18)

(iv) Mulroney's Plan to "Neutralize" Lumumba

After Mulroney arrived in the Congo, he formulated a plan for "neutralizing" Lumumba by drawing him away from the custody of the U.N. force which was guarding his residence:

MULRONEY: [W]hat I wanted to do was to get him out, to trick him out, if I could, and then turn him over *** to the legal authorities and let him stand trial. Because he had atrocity attributed to him for which he could very well stand trial.

Q: And for which he could very well have received capital punishment?

MULRONEY: Yes. And I am not opposed to capital punishment. (Mulroney, 9/11/75, pp. 20–21)[52]

To implement his plan, Mulroney made arrangements to rent "an observation post over the palace in which Lumumba was safely ensconced." He also made the acquaintance of a U.N. guard to recruit him for an attempt to lure Lumumba outside U.N. protective custody. (Mulroney, 6/9/75, p. 20; 9/11/75, p. 21) Mulroney said that he cabled progress reports to CIA Headquarters, and kept the Station Officer informed about his activities. (Mulroney, 9/11/75, pp. 26–27, 56)

Mulroney arranged for CIA agent QJ/WIN, to come to the Congo to work with him:

> What I wanted to use him for was *** counter-espionage. *** I had to screen the U.S. participation in this *** by using a foreign national whom we knew, trusted, and had worked with *** the idea was for me to use him as an alter ego. (Mulroney, 6/9/75, pp. 19–20)

In mid-November, two cables from Leopoldville urged CIA Headquarters to send QJ/WIN:

> LOCAL OPERATIONAL CIRCUMSTANCES REQUIRE IMMEDIATE EXPEDITION OF QJ/WIN TRAVEL TO LEOPOLDVILLE. (CIA Cable, Leopoldville to Director, 11/13/60; see also 11/11/60)

The cables did not explain the "operational circumstances."

---

[52] When Mulroney's mission to draw Lumumba out of the hands of the U.N. was described to C. Douglas Dillon, who was Undersecretary of State at that time, Dillon testified that it conformed to United States policy toward Lumumba. (Dillon, 9/21/75, p. 50)

According to an earlier report from the Station Officer, it was the view of the Special Representative of the Secretary General of the United Nations that arrest by Congolese authorities was "JUST A TRICK TO ASSASSINATE LUMUMBA." (CIA Cable, Station Officer to Director, 10/11/60) The Station Officer proceeded to recommend Lumumba's arrest in the same cable:

> STATION HAS CONSISTENTLY URGED [CONGOLESE] LEADERS ARREST LUMUMBA IN BELIEF LUMUMBA WILL CONTINUE BE THREAT TO STABILITY CONGO UNTIL REMOVED FROM SCENE.

(b) QJ/WIN's Mission in the Congo: November–December 1960

QJ/WIN was a foreign citizen with a criminal background, recruited in Europe. (Memo to CIA Finance Division, Re: Payments to QJ/WIN, 1/31/61) In November 1960, agent QJ/WIN was dispatched to the Congo to undertake a mission that "might involve a large element of personal risk." (CIA Cable, 11/2/60)[53]

A cable from Headquarters to Leopoldville stated:

> In view of the extreme sensitivity of the objective for which we want [QJ/WIN] to perform his task, he was not told precisely what we want him to do ∗∗∗. Instead, he was told ∗∗∗ that we would like to have him spot, assess, and recommend some dependable, quick-witted persons for our use ∗∗∗. It was thought best to withhold our true, specific requirements pending the final decision to use [him]. (CIA Cable, 11/2/60)

This message itself was deemed too sensitive to be retained at the station: "this dispatch should be reduced to cryptic necessary notes and destroyed after the first reading." (CIA Cable, 11/2/60)

QJ/WIN arrived in Leopoldville on November 21, 1960, and returned to Europe in late December 1960. (CIA Cable, 11/29/60; CIA Cable, Director to Leopoldville, 12/9/60)

Mulroney described QJ/WIN as follows:

MULRONEY: ∗∗∗ I would say that he would not be a man of many scruples.
Q: So he was a man capable of doing anything?
MULRONEY: I would think so, yes.
Q: And that would include assassination?
MULRONEY: I would think so. (Mulroney, 9/11/75, pp. 35–36)

But Mulroney had no knowledge that QJ/WIN was ever used for an assassination operation. (Mulroney, 9/11/75, pp. 36, 42)

Mulroney said that, as far as he knew, he was the only CIA officer with supervisory responsibility for QJ/WIN, and QJ/WIN did not report independently to anyone else. When asked if it was possible that QJ/WIN had an assignment independent of his operations for Mulroney, he said:

> Yes, that is possible—or it could have been that somebody contacted him after he got down there, that they wanted him to do something along the lines of assassination. I don't know. (Mulroney, 9/11/75, pp. 28, 29)

[53] An additional purpose in dispatching QJ/WIN was to send him from the Congo to another African country for an unspecified mission. QJ/WIN's mission to this country is not explained in the cable traffic between CIA Headquarters and the various stations that dealt with him.

There is no indication in CIA files as to whether QJ/WIN completed this operation. Mulroney said he had no knowledge of any assignment that would have taken QJ/WIN to this other country. (Mulroney, 9/11/75, pp. 32–33) William Harvey stated that he recalled that QJ/WIN might have been sent to an African country other than the Congo, but Harvey was "almost certain that this was not connected in any way to an assassination mission." (Harvey affidavit, 9/14/75, p. 5)

Mulroney discounted this possibility as "highly unlikely" because it would be a departure from standard CIA practice by placing an agent in a position of knowledge superior to that of his supervising officer. (Mulroney, 9/11/75, p. 29)

Despite Mulroney's doubt that QJ/WIN had an independent line of responsibility to Station Officer Hedgman, Hedgman's November 29 cable to Tweedy reported that QJ/WIN had begun implementing a plan to "pierce both Congolese and U.N. guards" to enter Lumumba's residence and "provide escort out of residence." (CIA Cable, Station Officer to Tweedy, 11/29/60) Mulroney said that he had directed QJ/WIN to make the acquaintance of the member of U.N. force. (Mulroney, 9/11/75, p. 21) By this point, Lumumba had already left U.N. custody to travel toward his stronghold at Stanleyville. This did not deter QJ/WIN:

> VIEW CHANGE IN LOCATION TARGET, QJ/WIN ANXIOUS GO STANLEYVILLE AND EXPRESSED DESIRE EXECUTE PLAN BY HIMSELF WITHOUT USING ANY APPARAT (CIA Cable, 11/29/60)

It is unclear whether this latter "plan" contemplated assassination as well as abduction. Headquarters replied affirmatively the next day in language which could have been interpreted as an assassination order:

> CONCUR QJ/WIN GO STANLEYVILLE ∗∗∗ WE ARE PREPARED CONSIDER DIRECT ACTION BY QJ/WIN BUT WOULD LIKE YOUR READING ON SECURITY FACTORS. HOW CLOSE WOULD THIS PLACE [UNITED STATES] TO THE ACTION? (CIA Cable, Chief of Africa Division to Station Officer, 11/30/60)

Mulroney said that QJ/WIN's stay in the Congo was "coextensive with my own, allowing for the fact that he came after I did." (Mulroney, 6/9/75, p. 19)

In a memorandum to arrange the accounting for QJ/WIN's activities in the Congo, William Harvey, Mulroney's immediate superior in the Directorate of Plans, noted: "QJ/WIN was sent on this trip for a specific, highly sensitive operational purpose which has been completed." (Memo for Finance Division from Harvey, 1/11/61) Mulroney explained Harvey's reference by saying that once Lumumba was in the hands of the Congolese authorities "the reason for the mounting of the project ∗∗∗ had become moot." When asked if he and QJ/WIN were responsible for Lumumba's departure from U.N. custody and subsequent capture, Mulroney replied: "Absolutely not." (Mulroney, 9/11/75, p. 35)[54]

Despite the suggestive language of the cables at the end of November about the prospect of "direct action" by QJ/WIN and an indication in the Inspector General's Report that QJ/WIN may have been recruited initially for an assassination mission[55] there is no clear evidence that QJ/WIN was actually involved in any assassination plan or attempt. The Inspector General's Report may have accurately reported a plan for the use of QJ/WIN

[54] Harvey did not recall the meaning of the memorandum, but he assumed that the mere fact that Mulroney had returned from the Congo would have constituted the "completion" of QJ/WIN's mission. (Harvey affidavit, 9/14/75, p. 2)

[55] The CIA Inspector General's Report said that QJ/ WIN "had been recruited earlier ∗∗∗ for use in a special operation in the Congo (the assassination of Patrice Lumumba) to be run by Michael Mulroney." (LG. Report, p. 38)

As explained above, Bissell and Mulroney testified that Mulroney had refused to be associated with an assassination operation. *See* sections 5(a) (ii) and (iii).

which predated Mulroney's refusal to accept the assassination assignment from Bissell. But there is no evidence from which to conclude that QJ/WIN was actually used for such an operation.

Station Officer Hedgman had a "vague recollection" that QJ/WIN was in the Congo working for Mulroney. But Hedgman did not recall why QJ/WIN was in the Congo and said that QJ/WIN was not one of his major operatives. (Hedgman, 8/21/75, p. 95) Bissell and Tweedy did not recall anything about QJ/WIN's activities in the Congo. (Bissell, 9/10/75, pp. 54–57; Tweedy, 9/9/75, pp. 54, 61)

Harvey, whose division "loaned" QJ/ WIN to the Congo Station, testified:

> I was kept informed of the arrangements for QJ/WIN's trip to the Congo and, subsequently, of his presence in the Congo. I do not know specifically what QJ/WIN did in the Congo. I do not think that I ever had such knowledge ∗∗∗. If QJ/WIN were to be used on an assassination mission, it would have been cleared with me. I was never informed that he was to be used for such a mission. (Harvey affidavit, 9/14/75, pp. 3–4)[56]

A 1962 CIA cable indicates the value the CIA accorded QJ/WIN and the inherent difficulty for an intelligence agency in employing criminals. The CIA had learned that QJ/WIN was about to go on trial in Europe on smuggling charges and Headquarters suggested:

> If ∗∗∗ INFOR[MATION] TRUE WE MAY WISH ATTEMPT QUASH CHARGES OR ARRANGE SOMEHOW SALVAGE QJ/WIN FOR OUR PURPOSES. (CIA Cable, 1962)

(c) WI/ROGUE Asks QJ/WIN to Join "Execution Squad": December 1960

The only suggestion that QJ/WIN had any connection with assassination was a report that WI/ROGUE, another asset of the Congo Station, once asked QJ/WIN to join an "execution squad."

WI/ROGUE was an "essentially stateless" soldier of fortune, "a forger and former bank robber." (Inspector General Memo, 3/14/75)[57] The CIA sent him to the Congo after providing him with plastic surgery and a toupee so that Europeans traveling in the Congo would not recognize him. (I.G. Memo, 3/14/75) The CIA characterized WI/ROGUE as a man who "learns quickly and carries out any assignment without regard for danger." (CIA Cable, Africa Division to Leopoldville, 10/27/60) CIA's Africa Division recommended WI/ROGUE as an agent in the following terms:

> He is indeed aware of the precepts of right and wrong, but if he is given an assignment which may be morally wrong in the eyes of the world, but necessary because his case officer ordered him to

[56] Harvey stated that the memoranda concerning QJ/WIN were probably written for his signature by the officer who supervised QJ/WIN's activities in Europe. (Harvey affidavit, 9/14/75, pp. 1, 4)

Harvey said that in later discussions he held with Scheider concerning the development of a general assassination capability, Scheider never mentioned QJ/WIN's activities in the Congo, nor did Scheider refer to his own trip to Leopoldville. Harvey also stated that before the formation of that project, QJ/WIN's case officer had not previously used him "as an assassination capability or even viewed him as such." (Harvey affidavit, 9/14/75, pp. 7, 8) *See* discussion in Part III, Section C.

[57] This information was derived from a report on WI/ROGUE'S assignment to the Congo prepared by a former Africa Division officer on March 14, 1975 at the request of the CIA Office of the Inspector General.

> carry it out, then it is right, and he will dutifully undertake appropriate action for its execution without pangs of conscience. In a word, he can rationalize all actions.

Station Officer Hedgman described WI/ROGUE as "a man with a rather unsavory reputation, who would try anything once, at least." Hedgman used him as "a general utility agent" because "I felt we needed surveillance capability, developing new contacts, various things." Hedgman supervised WI/ROGUE directly and did not put him in touch with Mulroney. (Hedgman, 8/21/75, pp. 96–97)

A report on agent WI/ROGUE, prepared for the CIA Inspector General's Office in 1975, described the training he received:

> On 19 September 1960 two members of Africa Division met with him to discuss "an operational assignment in Africa Division." In connection with this assignment, WI/ROGUE was to be trained in demolitions, small arms, and medical immunization. (I.G. Memo, 3/14/75)[58]

The report also outlined WI/ROGUE'S assignment to the Congo and recorded no mention of the use to which WI/ROGUE'S "medical immunization" training would be put:

> In October 1960 a cable to Leopoldville stated that * * * Headquarters [had] * * * intent to use him as utility agent in order to (a) organize and conduct a surveillance team; (b) intercept packages; (c) blow up bridges; and (d) execute other assignments requiring positive action. His utilization is not to be restricted to Leopoldville." (I.G. Memo, 3/14/75)

WI/ROGUE made his initial contact with Hedgman in Leopoldville on December 2, 1960. Hedgman instructed him to 'build cover during initial period;" and to "spot persons for [a] surveillance team" of intelligence agents in the province where Lumumba's support was strongest. (CIA Cable, 12/17/60)

Soon thereafter Hedgman cabled Headquarters:

> QJ/WIN WHO RESIDES SAME HOTEL AS WI/ROGUE REPORTED * * * WI/ROGUE SMELLED AS THOUGH HE IN INTEL BUSINESS. STATION DENIED ANY INFO ON WI/ROGUE. 14 DEC QJ/WIN REPORTED WI/ROGUE HAD OFFERED HIM THREE HUNDRED DOLLARS PER MONTH TO PARTICIPATE IN INTEL NET AND BE MEMBER "EXECUTION SQUAD." WHEN WI/ROGUE ADDED THERE WOULD BE BONUSES FOR SPECIAL JOBS. UNDER QJ/WIN QUESTIONING, WI/ROGUE LATER SAID HE WORKING FOR [AMERICAN] SERVICE.
>
> * * * IN DISCUSSING LOCAL CONTACTS, WI/ROGUE MENTIONED QJ/WIN BUT DID NOT ADMIT TO HAVING TRIED RECRUIT HIM. WHEN [STATION OFFICER] TRIED LEARN WHETHER WI/ROGUE HAD MADE APPROACH LATTER CLAIMED HAD TAKEN NO STEPS. [STATION OFFICER] WAS UNABLE CONTRADICT, AS DID NOT WISH REVEAL QJ/WIN CONNECTION [WITH CIA]. (CIA Cable, Leopoldville to Director, 12/17/60)

---

[58] A case officer who prepared WI/ROGUE for his mission in the Congo stated that he had no knowledge that WI/ROGUE received any training in "medical immunization." The case officer assumed that an unclear cable reference to the fact that WI/ROGUE received innoculations before his journey was misinterpreted in the memorandum prepared for the Inspector General's Office on March 14, 1975. (WI/ROGUE Case Officer affidavit, 11/14/75)

The cable also expressed Hedgman's concern about WI/ROGUE's actions:

> *** LEOP CONCERNED BY WI/ROGUE FREE WHEELING AND LACK SECURITY. STATION HAS ENOUGH HEADACHES WITHOUT WORRYING ABOUT AGENT WHO NOT ABLE HANDLE FINANCES AND WHO NOT WILLING FOLLOW INSTRUCTIONS. IF HQS DESIRES, WILLING KEEP HIM ON PROBATION, BUT IF CONTINUE HAVE DIFFICULTIES, BELIEVE WI/ROGUE RECALL BEST SOLUTION. (CIA Cable, Leopoldville to Director, 12/17/60)

Hedgman explained WI/ROGUE's attempt to recruit QJ/WIN for an execution squad as an unauthorized unexpected contact. He testified that he had not instructed WI/ROGUE to make this kind of proposition to QJ/WIN or anyone else:

> I would like to stress that I don't know what WI/ROGUE was talking about as an "execution squad," and I am sure he was never asked to go out and execute anyone. (Hedgman, 8/21/75, p. 100)

Hedgman suggested that WI/ROGUE had concocted the idea of an execution squad:

> His idea of what an intelligence operative should do, I think, had been gathered by reading a few novels or something of the sort. (Hedgman, 8/21/75, p. 100)

Mulroney said he knew of no attempt by anyone connected with the CIA to recruit an execution squad and he did not remember WI/ROGUE. (Mulroney, 9/11/75, pp. 39–42) He stated that QJ/WIN was considered for use on "strong arm squad[s]," unrelated to assassinations:

> Surveillance teams where you have to go into crime areas *** where you need a fellow that if he gets in a box can fight his way out of it. (Mulroney, 9/11/75, p. 36)

Richard Bissell recalled nothing about WI/ROGUE's approach to QJ/WIN. (Bissell, 9/11/75, p. 71) Bronson Tweedy remembered that WI/ROGUE was "dispatched on a general purpose mission" to the Congo. But Tweedy testified that WI/ROGUE would "absolutely not" have been used on an assassination mission against Lumumba because " he was basically dispatched, assessed and dealt with by the balance of the Division" rather than by the two people in the Africa Division, Tweedy and his Deputy, who would have known that the assassination of Lumumba was being considered. (Tweedy, 9/9/75, pp. 63–65)

The Station Officer said that if WI/ROGUE had been involved in an actual assassination plan, he would have transmitted messages concerning WI/ROGUE in the PROP channel. Instead, he limited distribution of the cable about WI/ROGUE in a routine manner—as a CIA officer would "normally do *** when you speak in a derogatory manner of an asset." (Hedgman, 8/21/75, pp. 101–102)

Hedgman maintained that WI/ROGUE's proposition to QJ/WIN to join an "execution squad" could be attributed to WI/ROGUE's "freewheeling" nature:

> I had difficulty controlling him in that he was not a professional intelligence officer as such. He seemed to act on his own without seeking guidance or authority *** I found he was rather an unguided missile *** the kind of man that could get you in trouble before you knew you were in trouble. (Hedgman, 8/21/75, pp. 96–97)

But Hedgman did not disavow all responsibility for WI/ROGUE's actions:

> [I]f you give a man an order and he carries it out and causes a problem for the Station, then you accept responsibility. (Hedgman, 8/21/75, p. 97)

In sum, the testimony of the CIA officers involved in the PROP operation and the concern about WI/ROGUE'S "freewheeling" in Hedgman's cable suggests that agent WI/ROGUE's attempt to form an "execution squad" was an unauthorized, maverick action, unconnected to any CIA operation. However, the fact that WI/ROGUE was to be trained in "medical immunization" (I.G. Report Memo, 3/14/75) precludes a definitive conclusion to that effect.

6. The Question of Whether the CIA Was Involved in Bringing About Lumumba's Death in Katanga Province

The CIA officers most closely connected with the plot to poison Lumumba testified uniformly that they knew of no CIA involvement in Lumumba's death. The Congo Station had advance knowledge of the central government's plan to transport Lumumba into the hands of his bitterest enemies, where he was likely to be killed. But there is no evidentiary basis for concluding that the CIA conspired in this plan or was connected to the events in Katanga that resulted in Lumumba's death.

(a) Lumumba's Imprisonment After Leaving U.N. Custody: November 27–December 3, 196

The only suggestion that the CIA may have been involved in the capture of Lumumba by Mobutu's troops after Lumumba left U.N. custody on November 27, is a PROP cable from the Station Officer to Tweedy on November 14. The cable stated that a CIA agent had learned that Lumumba's

> POLITICAL FOLLOWERS IN STANLEYVILLE DESIRE THAT HE BREAK OUT OF HIS CONFINEMENT AND PROCEED TO THAT CITY BY CAR TO ENGAGE IN POLITICAL ACTIVITY. *** DECISION ON BREAKOUT WILL PROBABLY BE MADE SHORTLY. STATION EXPECTS TO BE ADVISED BY [AGENT] OF DECISION WAS MADE. *** STATION HAS SEVERAL POSSIBLE ASSETS TO USE IN EVENT OF BREAKOUT AND STUDYING SEVERAL PLANS OF ACTION. (CIA Cable, Station Officer to Tweedy, 11/14/60)

There is no other evidence that the CIA actually learned in advance of Lumumba's plan to depart for Stanleyville. In fact, a cable from Leopoldville on the day after Lumumba's escape evidenced the Station's complete ignorance about the circumstances of Lumumba's departure. (CIA Cable, Leopoldville to Director, 11/28/60) However, the same cable raises a question concerning whether the CIA was involved in Lumumba's subsequent capture en route by Congolese troops:

> [STATION] WORKING WITH [CONGOLESE GOVERNMENT] TO GET ROADS BLOCKED AND TROOPS ALERTED [BLOCK] POSSIBLE ESCAPE ROUTE. (CIA Cable, 11/28/60)

Station Officer Hedgman testified that he was "quite certain that there was no Agency involvement in any way" in Lumumba's departure from U.N. custody and that he had no advance knowledge of Lumumba's plan. He stated that he consulted with Congolese

officers about the possible routes Lumumba might take to Stanleyville, but he was "not a major assistance" in tracking down Lumumba prior to his capture. (Hedgman, 8/21/75, pp. 63–65)

Mulroney, who had planned to draw Lumumba out of U.N. custody and turn him over to Congolese authorities, testified that Lumumba escaped by his own devices and was not tricked by the CIA. (Mulroney, 9/11/75, p. 22)

(b) Lumumba's Death

The contemporaneous cable traffic shows that the CIA was kept informed of Lumumba's condition and movements in January of 1961 by the Congolese and that the CIA continued to consider Lumumba a serious political threat. Despite the fact that the Station Officer knew of a plan to deliver Lumumba into the hands of his enemies at a time when the CIA was convinced that "drastic steps" were necessary to prevent Lumumba's return to power, there is no evidence of CIA involvement in this plan or in bringing about the death of Luntumba in Katanga.

There is no doubt that the CIA and the Congolese government shared a concern in January 1961 that Lumumba might return to power, particularly since the Congolese army and police were threatening to mutiny if they were not given substantial pay raises. Station Officer Hedgman reported that a mutiny "almost certainly would * * * bring about [Lumumba] return power" and said he had advised the Congolese government of his opinion that the army garrison at Leopoldville

> WILL MUTINY WITHIN TWO OR THREE DAYS UNLESS DRASTIC ACTION TAKEN SATISFY COMPLAINTS. (CIA Cable, Leopoldville to Director, 1/12/61)

Hedgman urged Headquarters to consider an immediate reaction to the crisis. (CIA Cable, 1/12/61) This cable, which was sent through the ordinary channel, made no reference, even indirectly, to assassination, and instead recommended a different course of action.

The next day, Hedgman cabled Headquarters:

> STATION AND EMBASSY BELIEVE PRESENT GOVERNMENT MAY FALL WITHIN FEW DAYS. RESULT WOULD ALMOST CERTAINLY BE CHAOS AND RETURN [LUMUMBA] TO POWER. (CIA Cable, Leopoldville to Director, 1/13/61)

Hedgman advised that reopening the Congolese Parliament under United Nations supervision was unacceptable because:

> THE COMBINATION OF [LUMUMBA'S] POWERS AS DEMAGOGUE, HIS ABLE USE OF GOON SQUADS AND PROPAGANDA AND SPIRIT OF DEFEAT WITHIN [GOVERNMENT] COALITION WHICH WOULD INCREASE RAPIDLY UNDER SUCH CONDITIONS WOULD ALMOST CERTAINLY INSURE [LUMUMBA] VICTORY IN PARLIAMENT. * * * REFUSAL TAKE DRASTIC STEPS AT THIS TIME WILL LEAD TO DEFEAT OF [UNITED STATES] POLICY IN CONGO. (CIA Cable, Leopoldville to Director, 1/13/61)

On January 14, Hedgman was advised by a Congolese government leader that Lumumba was to be transferred from the Thysville military camp, where he had been held since shortly after Mobutu's troops captured him, to a prison in Bakwanga, the capital of another Congolese province reported to be the "home territory of * * * Lumumba's sworn enemy." (CIA Cable, Leopoldville to Director, 1/17/61; CIA Information Report, 1/17/61)

On January 17, authorities in Leopoldville placed Lumumba and two of his leading supporters, Maurice Mpolo and Joseph Okito aboard an airplane bound for Bakwanga. Appparently the aircraft was redirected in midflight to Elisabethville in Katanga Province "when it was learned that United Nations troops were at Bakwanga airport." On February 13, the government of Katanga reported that Lumumba and his two companions escaped the previous day and died at the hands of hostile villagers. (U.N. Report, 11/12/61, pp. 98–100; 109)

The United Nations Commission on Investigation was "not convinced by the version of the facts given by the provincial government of Katanga." The Commission concluded instead, that Lumumba was killed on January 17, almost immediately after his arrival in Katanga, probably with the knowledge of the central government and at the behest of the Katanga authorities. (U.N. Report, 11/11/61, pp. 100, 117):

> The Commission wishes to put on record its view that President Kasavubu and his aides, on the one hand, and the provincial government of Katanga headed by Mr. Tshombe on the other, should not escape responsibility for the death of Mr. Lumumba, Mr. Okito, and Mr. Mpolo. For Mr. Kasavubu and his aides had handed over Mr. Lumumba and his colleagues to the Katanga authorities knowing full well, in doing so, that they were throwing them into the hands of their bitterest political enemies. The government of the province of Katanga in turn not only failed to safeguard the lives of the three prisoners but also had, by its action, contributed, directly or indirectly, to the murder of the prisoners. (U.N. Report, 11/11/61, p. 118)

Cables from the Station Officer demonstrated no CIA involvement in the plan to transport Lumumba to Bakwanga. But the Station Officer clearly had prior knowledge of the plan to transfer Lumumba to a state where it was probable that he would be killed. Other supporters of Lumumba who had been sent to Bakwanga earlier by Lepoldville authorities

> Were killed there in horrible circumstances, and the place was known as the 'slaughterhouse.' It was therefore improbable that Mr. Lumumba and his companions would have met a different fate at Bakwanga if they had been taken there. (U.N. Report, 11/11/61, p. 109)

After learning that Lumumba was to be flown to Bakwanga, the Station Officer cabled:

> IT NOW MORE IMPORTANT THAN EVER SUPPORT THOSE SINGLE ELEMENTS WHICH CAN STRENGTHEN FABRIC OVERALL * * * OPPOSITION [LUMUMBA]. WISH ASSURE HQS WE TRYING SHORE UP * * * DEFENSES ONLY IN TERMS OUR OWN OBJECTIVES DENY CONGO GOVT CONTROL [LUMUMBA]. (CIA Cable, 1/16/61)

Despite his perception of an urgent need to prevent Lumumba's return to power at this time, the Station Officer testified that the CIA was not involved in bringing about Lumumba's death in Katanga and that he did not have any first-hand knowledge of the circumstances of Lumumba's death. (Hedgman, 8/25/75, pp. 31, 33)[59]

[59] Hedgman also testified that he had no discussions with the Congolese central government, after Lumumba was in its custody, about executing Lumumba or sending him to Katanga. Hedgman said:

To the best of my knowledge, neither the Station nor the Embassy had any input in the decision to send him to Katanga * * * I think there was a general assumption, once we learned he had been sent to Katanga, that his goose was cooked, because Tshombe hated him and looked on him as a danger and rival. (Hedgman, 8/21/75, p. 78)

In late November, Hedgman attended a meeting of CIA officers from African Stations with Bissell and Tweedy. Hedgman testified that he briefed Bissell and Tweedy on developments in the Congo, including Lumumba's flight from Leopoldville, but he could not recall any discussion at the meeting of the possibility of assassinating Lumumba. (Hedgman, 8/21/75, pp. 66, 68)

Two days after Lumumba was flown to Katanga, the CIA Base Chief in Elisabethville sent an unusual message to headquarters:

> THANKS FOR PATRICE. IF WE HAD KNOWN HE WAS COMING WE WOULD HAVE BAKED A SNAKE.

The cable also reported that the Base's sources had provided "no advance word whatsoever" of Lumumba's flight to Katanga and that the Congolese central government "does not plan to liquidate Lumumba." (CIA Cable, Elisabethville to Director, 1/19/61)

This cable indicates that the CIA did not have knowledge of the central government's decision to transfer Lumumba from Thysville military camp to a place where he would be in the hands of his avowed enemies. This cable indicates that the CIA was not kept informed of Lumumba's treatment after he arrived in Katanga because, according to the report of the United Nations Commission, Lumumba had already been killed when the cable was sent.[60]

On February 10, several weeks after Lumumba died, but before his death was announced by the Katanga government, the Elisabethville Base cabled Headquarters that "Lumumba fate is best kept secret in Katanga." (CIA Cable, Elisabethville to Director, 2/10/61) The cable gave different versions from several sources about Lumumba's death. Hedgman testified that the cable conformed to his recollection that the CIA "did not have any hard information" as of that date about Lumumba's fate after arrival in Katanga. (Hedgman, 8/25/75, p. 34)

Hedgman acknowledged that the CIA was in close contact with some Congolese officials who "quite clearly knew" that Lumumba was to be shipped to Katanga "because they were involved." But Hedgman said that these Congolese contacts "were not acting under CIA instructions if and when they did this." (Hedgman, 8/21/75, p. 35)

Tweedy and Mulroney agreed with Hedgman's account that the CIA was not involved in the events that led to Lhmumba's death.[61]

7. The Question of The Level at Which The Assassination Plot Was Authorized

SUMMARY

The chain of events revealed by the documents and testimony is strong enough to permit a reasonable inference that the plot to assassinate Lumumba was authorized by

[60] Hedgman testified that neither he nor the Elisabethville Base knew of a Congolese plan to send Lumumba to Katanga. (Hedgman, 8/25/75, pp. 25–26)

[61] When asked if there was any CIA involvement, Tweedy replied that there was "none whatsoever." Tweedy stated that "the fate of Lumumba in the end was purely an African event." (Tweedy, 9/9/75, p. 53) Mulroney testified "CIA had absolutely no connection, to my certain knowledge, with the death of Patrice Lumumba." (Mulroney, 6/9/75, p. 20)

During his tenure as DCI, several years after Lumumba's death, Richard Helms was told by CIA investigators that "it was clear that the Agency had not murdered Lumumba," and that "the Agency had no involvement" in the events that led to Lumumba's death. (Helms, 9/16/75, p. 26)

President Eisenhower. Nevertheless, there is enough countervailing testimony by Eisenhower Administration officials and enough ambiguity and lack of clarity in the records of high-level policy meetings to preclude the Committee from making a finding that the President intended an assassination effort against Lumumba.

It is clear that the Director of Central Intelligence, Allen Dulles, authorized an assassination plot. There is, however, no evidence of United States involvement in bringing about the death of Lumumba at the hands of Congolese authorities in Katanga.

Strong expressions of hostility toward Lumumba from the President and his national security assistant, followed immediately by CIA steps in furtherance of an assassination operation against Lumumba, are part of a sequence of events that, at the least, make it appear that Dulles believed assassination was a permissible means of complying with pressure from the President to remove Lumumba from the political scene.

The chain of significant events in the Lumumba case begins with the testimony that President Eisenhower made a statement at a meeting of the National Security Council in the summer or early fall of 1960 that came across to one staff member in attendance as an order for the assassination of Patrice Lumumba. The next link is a memorandum of the Special Group meeting of August 25, 1960, which indicated that when the President's "extremely strong feelings on the necessity for very straightforward action" were conveyed, the Special Group

> * * * agreed that planning for the Congo would not necessarily rule out "consideration" of any particular kind of activity which might contribute to getting rid of Lumumba. (Special Group Minutes, 8/25/60)

The following day, CIA Director Allen Dulles, who had attended the Special Group meeting, personally cabled to the Station Officer in Leopoldville that Lumumba's

> REMOVAL MUST BE AN URGENT AND PRIME OBJECTIVE * * * A HIGH PRIORITY OF OUR COVERT ACTION. YOU CAN ACT ON YOUR OWN AUTHORITY WHERE TIME DOES NOT PERMIT REFERRAL HERE. (CIA Cable, Dulles to Station Officer, 8/26/60)

Although the Dulles cable does not explicitly mention assassination, Richard Bissell—the CIA official under whose aegis the assassination effort against Lumumba took place—testified that, in his opinion, this cable was a direct outgrowth of the Special Group meeting and signaled to him that the President had authorized assassination as one means of effecting Lumumba's "removal." (Bissell, 9/10/75, pp. 33–34 61–62; see Section 7(c), *infra*) Bronson Tweedy, who had direct operational responsibility at Headquarters for activities against Lumumba, testified that the Dulles cable confirmed the policy that no measure, including assassination, was to be overlooked in the attempt to remove Lumumba from a position of influence. (Tweedy, 10/9/75, pp. 4–5)

On September 19, 1960, Bissell and Tweedy cabled Station Officer Hedgman to expect a messenger from CIA Headquarters. Two days later, in the presence of the President at a meeting of the National Security Council, Allen Dulles stated that Lumumba "would remain a grave danger as long as he was not yet disposed of." (Memorandum, 460th NSC Meeting, 9/21/60) Five days after this meeting, CIA scientist, Joseph Scheider, arrived in Leopoldville and provided the Station Officer with toxic biological substances, instructed

him to assassinate Lumumba, and informed him that the President had authorized this operation.

Two mitigating factors weaken this chain just enough so that it will not support an absolute finding of Presidential authorization for the assassination effort against Lumumba.

First, the two officials of the Eisenhower Administration responsible to the President for national security affairs and present at the NSC meetings in question testified that they knew of no Presidential approval for, or knowledge of, an assassination operation.

Second, the minutes of discussions at meetings of the National Security Council and its Special Group do not record an explicit Presidential order for the assassination of Lumumba. The Secretary of the Special Group maintained that his memoranda reflected the actual language used at the meetings without omission or euphemism for extremely sensitive statements. (Parrott, 7/10/75, p. 19) All other NSC staff executives stated however, that there was a strong possibility that a statement as sensitive as an assassination order would have been omitted from the record or handled by means of euphemism. Several high Government officials involved in policymaking and planning for covert operations testified that the language in these minutes clearly indicated that assassination was contemplated at the NSC as one means of eliminating Lumumba as a political threat; other officials testified to the contrary.

(a) High-Level Meetings at which "Getting Rid of Lumumba" Was Discussed

(i) Dillon's Testimony About Pentagon Meeting: Summer 1960

In late July 1960, Patrice Lumumba visited the United States and met with Secretary of State Christian Herter and Undersecretary of State C. Douglas Dillon. While Lumumba was in Washington, D.C., Secretary Herter pledged aid to the newly formed Government of the Republic of the Congo.

According to Dillon, Lumumba impressed American officials as an irrational, almost "psychotic" personality:

> When he was in the State Department meeting, either with me or with the Secretary in my presence * * * he would never look you in the eye. He looked up at the sky. And a tremendous flow of words came out. He spoke in French, and he spoke it very fluently. And his words didn't ever have any relation to the particular things that we wanted to discuss * * *. You had a feeling that he was a person that was gripped by this fervor that I can only characterize as messianic * * *. [H]e was just not a rational being. (Dillon, 9/2/75, p. 24)

Dillon said that the willingness of the United States government to work with Lumumba vanished after these meetings:

> [T]he impression that was left was * * * very bad, that this was an individual whom it was impossible to deal with. And the feelings of the Government as a result of this sharpened very considerably at that time * * *. We [had] hoped to see him and see what we could do to come to a better understanding with him. (Dillon, 9/2/75, pp. 23–24)

Dillon testified that shortly after Lumumba's visit in late July or August, he was present at a meeting at the Pentagon attended by representatives of the State Department, Defense Department, Joint Chiefs of Staff and the CIA. (Dillon, 9/2/75, pp. 17–20, 25–26)[62]

[62] Dillon was unable to recall the precise date of this meeting. (Dillon, 9/2/75, pp. 25–26)

According to Dillon, "a question regarding the possibility of an assassination attempt against Lumumba was briefly raised. Dillon did not recall anything about the language used in raising the question. Dillon assumed that when the subject of Lumumba's assassination was raised, "it was turned off by the CIA" because "the CIA people, whoever they were, were negative to any such action." This opposition "wasn't moral," according to Dillon, but rather an objection on the grounds that it was "not a possible thing." Dillon said the CIA reaction "might have been" made out of the feeling that the group was too large for such a sensitive discussion. (Dillon, 9/2/75, pp. 15–17, 25, 30, 60)

Dillon did not remember who lodged the negative reaction to the assassination question although he thought it "would have to have been either Allen Dulles, or possibly [General] Cabell * * * most likely Cabell."[63] (Dillon, 9/2/75, pp. 22, 25) Dillon thought it was "very likely that Richard Bissell attended the meeting. (Dillon, 9/2/75, p. 21)

Dillon stated that this discussion could not have served as authorization for an actual assassination effort against Lumumba, but he believed that the CIA:

> Could have decided they wanted to develop the capability * * * just by knowing the concern that everyone had about Lumumba. * * * They wouldn't have had to tell anyone about that. That is just developing their own internal capability, and then they would have to come and get permission. (Dillon, 9/2/75, pp. 30, 31)

Dillon testified that he had never heard any mention of the plot to poison Lumumba nor, even a hint that the CIA asked permission to mount such an operation. (Dillon, 9/2/75, p. 50) But after he was informed of the poison plot, Dillon made the following comment about the Pentagon meeting:

> I think it is * * * likely that it might have been the beginning of this whole idea on the CIA's part that they should develop such a capacity. And maybe they didn't have it then and went to work to develop it beginning in August. (Dillon, 9/2/75, p. 61)

Dillon said that it was unlikely that formal notes were taken at the meeting or preserved because it was a small "ad hoc" group rather than an official body. Such interdepartmental meetings were "not unusual," according to Dillon. (Dillon, 9/2/75, p. 18)

The only officials Dillon named as probable participants other than the CIA representatives were Deputy Secretary of Defense James Douglas and Assistant Secretary of Defense John N. Irwin II. (Dillon, 9/2/75, pp. 19, 21) Douglas stated that it was possible that he attended such a meeting at the Pentagon, but he did not recall it. Nor did he recall the question of Lumumba's assassination ever being raised in his presence. (Douglas affidavit, 9/5/75) Irwin stated that it was "likely" that he attended the meeting to which Dillon referred, but he did not remember whether he was present "at any meeting at the Pentagon where the question of assassinating Patrice Lumumba was raised." (Irwin affidavit, 9/22/75, p. 3)

(ii) Robert Johnson's Testimony That He Understood the President to Order Lumumba's Assassination at an NSC Meeting

Robert H. Johnson, a member of the National Security Council staff from 1951 to January 1962, offered what he termed a "clue" to the extent of Presidential involvement in

[63] General Cabell was Allen Dulles' Deputy DCI at this time.

the decision to assassinate Lumumba. (Johnson, 6/18/75, pp. 4–5)[64] Johnson recounted the following occurrence at an NSC meeting, in the summer of 1960, which began with a briefing on world developments by the DCI:

> At some time during that discussion, President Eisenhower said something—I can no longer remember his words—that came across to me as an order for the assassination of Lumumba who was then at the center of political conflict and controversy in the Congo. There was no discussion; the meeting simply moved on. I remember my sense of that moment quite clearly because the President's statement came as a great shock to me. I cannot, however, reconstruct the moment more specifically.
>
> Although I was convinced at the time—and remained convinced when I thought about it later—that the President's statement was intended as an order for the assassination of Lumumba, I must confess that in thinking about the incident more recently I have had some doubts. As is well known, it was quite uncharacteristic of President Eisenhower to make or announce policy decisions in NSC meetings. Certainly, it was strange if he departed from that normal pattern on a subject so sensitive as this. Moreover, it was not long after this, I believe, that Lumumba was dismissed as premier by Kasavubu in an action that was a quasi-coup. I have come to wonder whether what I really heard was only an order for some such political action. All I can tell you with any certainty at the present moment is my sense of that moment in the Cabinet Room of the White House. (Johnson, 6/18/75, pp. 6–7)

Johnson "presumed" that the President made his statement while "looking toward the Director of Central Intelligence." (Johnson, 6/18/75, p. 11) He was unable to recall with any greater specificity the words used by the President. (Johnson, 9/13/75, p. 10) Johnson was asked:

Q: ∗∗∗ Would it be fair to say that although you allow for the possibility that a coup or some more general political action was being discussed, it is your clear impression that you had heard an order for the assassination of Lumumba?

JOHNSON: It was my clear impression at the time.

Q: And it remains your impression now?

---

[64] Robert Johnson introduced his testimony before the Committee with the following statement:

"∗∗∗ I would like to preface my remarks by pointing out that my decision to offer testimony to this committee has involved for me a profound personal, moral dilemma. In my role as a member of the NSC Staff for ten and one-half years, I was privy to a great deal of information that involved relationships of confidentiality with high officials of the United States government. I have always taken very seriously the responsibilities implied in such relationships.

"These responsibilities extend, in my view, far beyond questions of security classification or other legal or foreign policy concerns. They relate to the very basis of human society and government—to the relationships of trust without which no free society can long survive and no government can operate.

"I have been forced by recent developments, however to weigh against these considerable responsibilities, my broader responsibilities as a citizen on an issue that involves major questions of public morality, as well as questions of sound policy. Having done so, I have concluded, not without a great deal of reluctance, to come to your committee with information bearing upon your inquiry into government decisions relating to the assassination of foreign leaders." (Johnson, 6/18/75, pp. 4–5)

After his tenure on the staff of the National Security Council, Robert Johnson served from 1962 to 1967 on the Policy Planning Council at the Department of State.

JOHNSON: It remains my impression now. I have reflected on this other kind of possibility; but that is the sense * * * that persists. (Johnson, 9/13/75, pp. 24–25)[65]

Johnson stated that the incident provoked a strong reaction from him:

> I was surprised * * * that I would ever hear a President say anything like this in my presence or the presence of a group of people. I was startled. (Johnson, 6/18/75, p. 13)

A succinct summary of Johnson's testimony was elicited by Senator Mathias in the following exchange:

Senator MATHIAS: * * * What comes across is that you do have a memory, if not of exact words, but of your own reaction really to a Presidential order which you considered to be an order for an assassination.

JOHNSON: That is correct.

Senator MATHIAS: And that although precise words have escaped you in the passage of fifteen years, that sense of shock remains?

JOHNSON: Right. Yes, Sir. (Johnson, 6/18/75, p. 8)

After the meeting, Johnson, who was responsible for writing the memorandum of the discussion, consulted with a senior official on the NSC staff to determine how to handle the President's statement in the memorandum and in the debriefing of the NSC Planning Board that followed each meeting:

> I suspect—but no longer have an exact recollection—that I omitted it from the debriefing. I also do not recall how I handled the subject in the memo of the meeting, though I suspect that some kind of reference to the President's statement was made. (Johnson, 6/18/75, p. 7)

In his second appearance before the Committee, Johnson stated that it was "quite likely that it [the President's statement] was handled through some kind of euphemism or may have been omitted altogether." (Johnson, 9/13/75, p. 21)[66]

---

[65] Johnson further explained that his allowance for the possibility that he had heard an order for a coup did not disturb his recollection of hearing an assassination order:

"It was a retrospective reflection on what I had heard, and since this coup did occur, it occurred to me that it was possible that that is what I heard, but that would not change my sense of the moment when I heard the President speak, which I felt then, and I continue to feel, was a statement designed to direct the disposal, assassnation, of Lumumba." (Johnson, 9/13/75, p. 12)

[66] In 1960 Johnson was Director of the Planning Board Secretariat—third in command on the NSC staff. He attended NSC meetings to take notes on the discussions whenever one of the two senior NSC officials was absent.

Johnson testified that the person with whom he consulted about the manner of recording the President's statement in the minutes was one of the two top NSC staff officials at that time: NCS Executive Secretary James Lay or Deputy Executive Secretary Marion Boggs. (Johnson, 9/13/75, pp. 12–13) Johnson could not recall which of the two officials he had consulted, but he "inferred" that it must have been the "top career NSC staff person present" at the meeting where he heard the President's statement. (Johnson, 9/13/75, p. 12) At both of the NSC meetings where the President and Johnson were present for a discussion of Lumumba—August 18 and September 7—James Lay was absent and Marion Boggs served as Acting Executive Secretary.

As Johnson stated, his testimony standing alone is "a clue, rather than precise evidence of Presidential involvement in decision making with respect to assassinations." (Johnson, 6/18/75, p. 5) To determine the significance of this "clue," it must be placed in the context of the records of the NSC meetings attended by Johnson, testimony about those meetings, and the series of events that preceded the dispatch of poisons to the Congo for Lumumba's assassination.

In the summer of 1960, Robert Johnson attended four NSC meetings at which developments in the Congo were discussed. The President was not in attendance on two of those occasions—July 15 and July 21. (NSC Minutes, 7/15/60; NSC Minutes, 7/21/60) The attitude toward Lumumba at these first two meetings was vehement:

> Mr. Dulles said that in Lumumba we were faced with a person who was a Castro or worse * * * Mr. Dulles went on to describe Mr. Lumumba's background which he described as "harrowing" * * * It is safe to go on the assumption that Lumumba has been bought by the Communists; this also, however, fits with his own orientation. (NSC Minutes, 7/21/60)

The President presided over the other two NSC meetings—on August 18 and September 7. After looking at the records of those meetings, Johnson was unable to determine with certainty at which meeting he heard the President's statement.[67] (Johnson, 9/13/75, p. 16)

The chronology of meetings, cables, and events in the Congo during this period makes it most likely that Johnson's testimony refers to the NSC meeting of August 18, 1960.

The meeting of August 18 took place at the beginning of the series of events that preceded the dispatch of Scheider to Leopoldville with poisons for assassinating Lumumba.[68] The September 7 meeting took place in the midst of these events.

Marion Bogg's statement about his method of handling the situation described by Johnson is in accord with Johnson's testimony:

"I have no independent recollection of being consulted by Mr. Johnson about how to handle in the memorandum of discussion any sensitive statement regarding Lumumba. I am not saying I was not consulted; merely that I do not remember such an incident. If I had been consulted, I would almost certainly have directed Mr. Johnson to omit the matter from the memorandum of discussion." (Boggs affidavit, 10/10/75, p. 2)

James Lay, who attended other NSC meetings where Lumumba was discussed (*e.g.*, September 21, 1960), also confirmed the fact that NSC minutes would not be likely to record a statement as sensitive as a Presidential order for an assassination, if such an order were given:

"If extremely sensitive matters were discussed at an NSC meeting, it was sometimes the practice that the official NSC minutes would record only the general subject discussed without identifying the specially sensitive subject of the discussion. In highly sensitive cases, no reference to the subject would be made in the NSC minutes." (Lay affidavit, 9/8/75, p. 2)

[67] Johnson testified without benefit of review of the complete Memorandum of Discussion of the meeting of September 7 because the Committee had not received it at that point. Instead, he reviewed the Record of Action which summarized the decisions made at that meeting. As discussed at Section (7) (a) (iv), *infra,* when the complete minutes of the meetings of August 18 and September 7 are compared, it is clear that the subject of Lumumba's role in the Congo received far more attention at the meeting of August 18.

[68] Each of the major events in this series is discussed in detail in other sections of the report and summarized at the beginning of section 7, *supra.*

The NSC meeting of August 18, 1960 was held three weeks before Lumumba's dismissal by Kasavubu, which Johnson remembers as taking place "not long after" he heard the President's statement. The only other meeting at which Johnson could have heard the statement by the President was held two days after this event, on September 7.[69]

Robert Johnson's memorandum of the meeting of August 18, 1960 indicates that Acting Secretary of State C. Douglas Dillon[70] introduced the discussion of United States policy toward the Congo. In the course of his remarks, Dillon maintained that the presence of United Nations troops in the Congo was necessary to prevent Soviet intervention at Lumumba's request:

> If * * * Lumumba carried out his threat to force the U.N. out, he might then offer to accept help from anyone. * * * The elimination of the U.N. would be a disaster which, Secretary Dillon stated, we should do everything we could to prevent. If the U.N. were forced out, we might be faced by a situation where the Soviets intervened by invitation of the Congo.
>
> * * * Secretary Dillon said that he [Lumumba] was working to serve the purposes of the Soviets and Mr. Dulles pointed out that Lumumba was in Soviet pay. (NSC Minutes, 8/18/60)

Dillon's remarks prompted the only statements about Lumumba attributed to the President in the Memorandum of the August 18 meeting:

> The President said that the possibility that the U.N. would be forced out was simply inconceivable. We should keep the U.N. in the Congo even if we had to ask for European troops to do it. We should do so even if such action was used by the Soviets as the basis for starting a fight. Mr. Dillon indicated that this was State's feeling but that the Secretary General and Mr. Lodge doubted whether, if the Congo put up really determined opposition to the U.N., the U.N. could stay in. In response, the President stated that Mr. Lodge was wrong to this extent—we were talking of one man forcing us out of the Congo; of Lumumba supported by the Soviets. There was no indication, the President stated, that the Congolese did not want U.N. support and the maintenance of order. Secretary Dillon reiterated that this was State's feeling about the matter. The situation that would be created by a U. N. withdrawal was altogether too ghastly to contemplate. (NSC Minutes, 8/18/60)

As reported, this statement clearly does not contain an order for the assassination of Lumumba. But the statement does indicate extreme Presidential concern focused on Lumumba: the President was so disturbed by the situation in the Congo that he was willing to risk a fight with the Soviet Union and he felt that Lumumba was the "one man" who was responsible for this situation, a man who did not represent the sentiment of the Congolese people in the President's estimation.

After reviewing NSC documents and being informed of Robert Johnson's testimony, Douglas Dillon stated his "opinion that it is most likely that the NSC meeting of August 18,

---

[69] See Section 7(a) (iv), *infra*, for an analysis of the substance of the NSC discussion on September 7, 1960.

[70] In 1960, Dillon served as Undersecretary of State, the "number two position in the State Department." The title was subsequently changed to Deputy Secretary of State. In this post, Dillon frequently served as Acting Secretary of State and either attended or was kept informed about NSC and Special Group meetings. Dillon later served as Secretary of the Treasury under President Kennedy. (Dillon, 9/2/75, pp. 2–4)

1960 is the meeting referred to by Mr. Johnson." (Dillon affidavit, 9/15/75, p. 2) However, Dillon testified that he did not "remember such a thing" as a "clearcut order" from the President for the assassination of Lumumba. (Dillon, 9/2/75, pp. 32–33) Dillon explained how he thought the President may have expressed himself about Lumumba:

DILLON: It could have been in view of this feeling of everybody that Lumumba was [a] very difficult if not impossible person to deal with, and was dangerous to the peace and safety of the world, that the President expressed himself, we will have to do whatever is necessary to get rid of him. I don't know that I would have taken that as a clearcut order as Mr. Johnson apparently did. And I think perhaps others present may have interpreted it other ways. (Dillon, 9/2/75, pp. 32–33)

Q: Did you ever hear the President make such a remark about Lumumba, let's get rid of him, or let's take action right away on this?

DILLON: I don't remember that. But certainly this was the general feeling of Government at that time, and it wouldn't have been if the President hadn't agreed with it. (Dillon, 9/2/75, p. 33)

Dillon said that he would have thought that such a statement "was not a direct order to have an assassination." But he testified that it was "perfectly possible" that Allen Dulles would have translated such strong Presidential language about "getting rid of" Lumumba into authorization for an assassination effort. (Dillon, 9/2/75, pp. 33, 34–35):

> I think that Allen Dulles would have been quite responsive to what he considered implicit authorization, because he felt very strongly that we should not involve the President directly in things of this nature. And he was perfectly willing to take the responsibility personally that maybe some of his successors wouldn't have been. And so I think that this is a perfectly plausible thing, knowing Allen Dulles. (Dillon, 9/2/75, p. 34)

According to President Eisenhower's national security advisor, Gordon Gray, Dulles would have placed the CIA in a questionable position if he mounted an assassination operation on the basis of such "implicit authorization." Gray testified that the CIA would have been acting beyond its authority if it undertook an assassination operation without a specific order to do so. (Gray, 9/9/75, p. 18)

Marion Boggs, who attended the meeting of August 18, as Acting Executive Secretary of the NSC, stated after reviewing the Memorandum of Discussion at that Meeting:

> I recall the discussion at that meeting, but have no independent recollection of any statements or discussion not summarized in the memorandum. Specifically, I have no recollection of any statement, order or reference by the President (or anyone else present at the meeting) which could be interpreted as favoring action by the United States to bring about the assassination of Lumumba.[71] (Boggs affidavit, 10/10/75, pp. 1–2)

[71] Boggs added:

"Based on my whole experience with the NSC, I would have considered it highly unusual if a matter of this nature had been referred to in a Council meeting where a number of persons with no 'need to know' were present." (Boggs affidavit, 10/10/75, p. 2)

There are at least four possible explanations of the failure of NSC records to reveal whether the President ordered the assassination of Lumumba at one of the meetings where Robert Johnson was present.

First, an assassination order could have been issued but omitted from the records. Johnson testified that it was "very likely" that the Presidential statement he heard would have been handled by means of a euphemistic reference or by complete omission "rather than given as [a] * * * direct quotation" in the Memorandum of Discussion. (Johnson, 9/13/75, p. 14) NSC staff executives Marion Boggs and James Lay substantiated Johnson's testimony about the manner of handling such a statement in the records.

Second, as illustrated by Douglas Dillon's testimony, the President could have made a general statement about "getting rid of" Lumumba with the intent to convey to Allen Dulles implicit authorization for an assassination effort.

Third, despite general discussions about removing Lumumba, the President may not have intended to order the assassination of Lumumba even though Allen Dulles may have thought it had been authorized. The three White House staff members responsible to the President for national security affairs testified that there was no such order.[72]

Fourth, whatever language he used, the President may have intended to authorize "contingency planning" for an assassination effort against Lumumba, while reserving decision on whether to authorize an actual assassination attempt. This interpretation can be supported by a strict construction of the decision of the Special Group on August 25, in response to the "strong feelings" of the President, not to rule out " 'consideration' of any particular kind of activity which might contribute to getting rid of Lumumba" and by the testimony of Bronson Tweedy that the assassination operation was limited to "exploratory activity."[73]

(iii) Special Group Agrees to Consider Anything That Might Get Rid of Lumumba: August 25, 1960

On August 25, 1960, five men[74] attended a meeting of the Special Group, the subcommittee of the National Security Council responsible for planning covert operations. Thomas Parrott, a CIA officer who served as Secretary to the Group, began the meeting by outlining the CIA operations that had been undertaken in "mounting an anti-Lumumba campaign in the Congo." (Special Group Minutes, 8/25/60) This campaign involved covert operations through certain labor groups and "the planned attempt * * * to arrange a vote of no confidence in Lumumba" in the Congolese Senate. (Special Group Minutes, 8/25/60) The outline of this campaign evoked the followed dialogue:

---

[72] See Section 7 (b), *infra*, for a general treatment of the testimony of Gray, Goodpaster, and Eisenhower.

[73] This interpretation of the Special Group minutes must be posed against the testimony of other witnesses who construed the minutes as authorizing action, as well as planning an assassination operation. (Special Group Minutes, 8/25/60, p. 1; see Section 7 (a) (ii) *infra*) See Section 4 (h) (ii), *supra*, for a detailed discussion of Tweedy's testimony.

[74] The four standing members of the Special Group were in attendance: Allen Dulles, Director of Central Intelligence; Gordon Gray, Special Assistant to the President for National Security Affairs; Livingston Merchant, Undersecretary of State for Political Affairs; and John N. Irwin II, Assistant Secretary of Defense. Also in attendance was Thomas A. Parrott, Secretary to the Special Group.

> The Group agreed that the action contemplated is very much in order. Mr. Gray commented, however, that his associates had expressed extremely strong feelings on the necessity for very straightforward action in this situation, and he wondered whether the plans as outlined were sufficient to accomplish this. Mr. Dulles replied that he had taken the comments referred to seriously and had every intention of proceeding as vigorously as the situation permits or requires, but added that he must necessarily put himself in a position of interpreting instructions of this kind within the bounds of necessity and capability. It was finally agreed that planning for the Congo would not necessarily rule out "consideration" of any particular kind of activity which might contribute to getting rid of Lumumba. (Special Group Minutes, 8/25/60, p. 1)

Both Gordon Gray and Thomas Parrott testified that the reference to Gray's "associates" was a euphemism for President Eisenhower which was employed to preserve "plausible deniability" by the President of discussion of covert operations memorialized in Special Group Minutes. (Gray, 7/9/75, p. 27; Parrott, 7/10/75, pp. 8–9)

The four living participants at the meeting have all stated that they do not recall any discussion of or planning for the assassination of Lumumba. Gray said that he did not consider the President's desire for "very straightforward action" to include "any thought in his mind of assassination." Parrott testified to the same effect, maintaining that he would have recorded a discussion of assassination in explicit terms in the Special Group Minutes if such a discussion had taken place. (Gray, 7/9/75, pp. 27, 32; Parrott, 7/10/75, pp. 25–26; Merchant affidavit, 9/8/75, p. 1; Irwin affidavit, 9/22/75, pp. 1–2) John N. Irwin II acknowledged, however, that while he did not have "any direct recollection of the substance of that meeting," the reference in the minutes to the planning for "getting rid of Lumumba" was "broad enough to cover a discussion of assassination." (Irwin affidavit, 9/22/75, p. 2)

Irwin's interpretation was shared by Douglas Dillon and Richard Bissell who were not participants at this Special Group meeting but were involved in the planning and policy-making for covert operations in the Congo during this period.

As a participant in NSC meetings of this period, Dillon said that he would read the Special Group minutes of August 25 to indicate that assassination was within the bounds of the kind of activity that might be used to "get rid of" Lumumba. Dillon noted that the reference in the minutes to Dulles' statement that he "had taken the comments referred to seriously" probably pointed to the President's statement at the NSC meeting on August 18. (Dillon, 9/2/75, pp. 39–42) When asked whether the CIA would have the authority to mount an assassination effort against Lumumba on the basis of the discussion at the Special Group, Dillon said:

> They would certainly have the authority to plan. It is a close question whether this would be enough to actually go ahead with it. But certainly the way this thing worked, as far as I know, they didn't do anything just on their own. I think they would have checked back at least with the senior people in the State Department or the Defense Department. (Dillon, 9/2/75, p. 43)

Dillon said that if the CIA checked with the State Department, it might have done so in a way that would not appear on any record. (Dillon, 9/2/75, p. 43) Dillon added that "to protect the President as the public representative of the U.S. from any bad publicity in connection with this," Allen Dulles "wouldn't return to the President" to seek further approval if an assassination operation were mounted. (Dillon, 9/2/75, pp. 42–43)

Bissell stated that in his opinion the language of the August 25 Special Group Minutes indicated that the assassination of Lumumba was part of a general NSC strategy and was

within the CIA's mandate for removing Lumumba from the political scene. (Bissell, 9/10/75, pp. 29, 32) He added:

> The Agency had put a top priority, probably, on a range of different methods of getting rid of Lumumba in the sense of either destroying him physically, incapacitating him, or eliminating his political influence. (Bissell, 9/10/75, p. 29)

Bissell pointed to the Special Group Minutes of August 25 as a "prime example" of the circumlocutious manner in which a topic like assassination would be discussed by high government officials:

> When you use the language that no particular means were ruled out, that is obviously what it meant, and it meant that to everybody in the room. * * * Meant that if it had to be assassination, that that was a permissible means.
>
> You don't use language of that kind except to mean in effect, the Director is being told, get rid of the guy, and if you have to use extreme means up to and including assassination, go ahead. (Bissell, 9/10/75, pp. 32–33)

Bissell added that this message was, "in effect," being given to Dulles by the President through his representative, Gordon Gray. (Bissell, 9/10/75, p. 33)

(iv) Dulles Reminded by Gray of "Top-Level Feeling" That "Vigorous Action" Was Necessary in the Congo: September 7–8, 1960

The Memorandum of Discussion from the NSC meeting of September 7, 1960—the only other meeting at which Johnson could have heard the President's statement—records only a brief, general discussion of developments in the Congo. As part of Allen Dulles' introductory intelligence briefing on world events, the Memorandum contained his remarks on the situation in the Congo following Kasavubu's dismissal of Lumumba from the government. Neither the length nor the substance of the record of this discussion indicates that Lumumba's role in the Congo received the same intense consideration as the NSC had given it on August 18.[75] There is no record of any statement by the President during the September 7 discussion. (NSC Minutes, 9/7/60, p. 4–5)

In the course of Dulles' briefing, he expressed his continuing concern over the amount of personnel and equipment that was being sent to the Congo by the Soviet Union, primarily to aid Lumumba. Dulles concluded this part of his briefing with an observation that demonstrated that Lumumba's dismissal from the government had not lessened the extent to which he was regarded at the NSC as a potent political threat in any power struggle in the Congo:

> Mr. Dulles stated that Lumumba always seemed to come out on top in each of these struggles. (NSC Minutes, 9/7/60, p. 5)

At a Special Group Meeting the next day, Gordon Gray made a pointed reminder to Allen Dulles of the President's concern about the Congo:

[75] The NSC minutes of the meeting of September 7 deal with the discussion of the Congo in two pages. (NSC Minutes, 9/7/60, pp. 4–5). By comparison, the August 18 meeting required an extraordinarily lengthy (fifteen pages) summary of discussion on the Congo and related policy problems in Africa, indicating that this topic was the focal point of the meeting. (NSC Minutes, 8/18/60, pp. 1–15)

> Mr. Gray said that he hoped that Agency people in the field are fully aware of the top-level feeling in Washington that vigorous action would not be amiss. (Special Group Minutes, 9/8/60)

(v) Dulles Tells NSC That Lumumba Remains a Grave Danger Until "Disposed of": September 21, 1960

In the course of his intelligence briefing to the NSC on September 21, 1960, Allen Dulles stressed the danger of Soviet influence in the Congo. Despite, the fact that Lumumba had been deposed as Premier and was in U.N. custody, Dulles continued to regard him as a threat, especially in light of reports of an impending reconciliation between Lumumba and the post-coup Congolese government. In the presence of the President, Dulles concluded:

> Mobutu appeared to be the effective power in the Congo for the moment but Lumumba was not yet disposed of and remained a grave danger as long as he was not disposed of. (NSC Minutes, 9/21/60)

Three days after this NSC meeting, Dulles sent a personal cable to the Station Officer in Leopoldville which included the following message:

> WE WISH GIVE EVERY POSSIBLE SUPPORT' IN ELIMINATING LUMUMBA FROM ANY POSSIBILITY RESUMING GOVERNMENTAL POSITION OR IF HE FAILS IN LEOP[OLDVILLE], SETTING HIMSELF IN STANLEYVILLE OR ELSEWHERE (CIA Cable, Dulles, Tweedy to Leopoldville, 9/24/60)

On September 26, Joseph Scheider, under assignment from CIA Headquarters, arrived in Leopoldville, provided the Station Officer with poisons, conveyed Headquarters' instruction to assassinate Lumumba, and assured him that there was Presidential authorization for this mission.[76]

Marion Boggs, the NSC Deputy Executive Secretary, who wrote the Memorandum of Discussion of September 21, did not interpret Dulles' remark as referring to assassination:

> I have examined the memorandum (which I prepared) summarizing the discussion of the Congo at the September 21, 1960 meeting of the NSC. I recall the discussion and believe it is accurately and adequately summarized in the memorandum. I have no recollection of any discussion of a possible assassination of Lumumba at this meeting. With specific reference to the statement of the Director of Central Intelligence * * * I believe this is almost a literal rendering of what Mr. Dulles said. My own interpretation of this statement * * * was that Mr. Dulles was speaking in the context of efforts being made within the Congolese government to force Lumumba from power. I did not interpret it as referring to assassination.[77] (Boggs affidavit, 10/10/75, pp. 2–3)

Boggs, however, was not in a position to analyze Dulles' remark in the context of the actual planning for covert operations that took place during this period because Boggs was not privy to most such discussions. (Boggs affidavit, 10/10/75, p. 2)

---

[76] See Sections 4(e)–4(f), *supra.*

[77] NSC Executive Secretary James Lay, who was also present at the meeting of September 21, 1960, stated: "I cannot recall whether there was any discussion of assassinating Lumumba at any NSC meetings." (Lay affidavit, 9/8/75, p. 1)

Dillon, who attended this NSC meeting as Acting Secretary of State, did not recall the discussion. Dillon said that the minutes "could mean that" assassination would have been one acceptable means of "disposing of" Lumumba, although he felt that "getting him out [of the Congo] or locking him up" would have been a preferable disposition of Lumumba at that point since he was already out of office. (Dillon, 9/2/75, pp. 47–48)[78] When reminded of the fact that Lumumba's movement and communications were not restricted by the U.N. force and that the Congolese army continued to seek his arrest after the September 21 meeting, Dillon acknowledged that during this period Lumumba continued to be viewed by the United States as a potential threat and a volatile force in the Congo:

> * * * He had this tremendous ability to stir up a crowd or a group. And if he could have gotten out and started to talk to a battalion of the Congolese Army, he probably would have had them in the palm of his hand in five minutes. (Dillon, 9/20/75, p. 49)

Irwin, who attended the NSC meeting as Assistant Secretary of Defense, stated that although he had no recollection of the discussion, the language of these minutes, like that of the August 25 minutes, was "broad enough to cover a discussion of assassination." (Irwin affidavit, 9/22/75, p. 2)

Bissell testified that, based upon his understanding of the policy of the NSC toward Lumumba even after Lumumba was in U.N. custody, he would read the minutes of September 21 to indicate that assassination was contemplated "as one possible means" of "disposing of" Lumumba[79] (Bissell, 9/10/75, p. 70)

Bissell's opinion stands in opposition to Gordon Gray's testimony. Gray stated that he could not remember the NSC discussion, but he interpreted the reference to "disposing of" Lumumba as "in the same category as 'get rid of,' 'eliminate'." (Gray, 7/9/75, p. 59) He said: "It was not my impression that we had in mind the assassination of Lumumba.") (Gray, 7/9/75, p. 60)[80]

(b) Testimony of Eisenhower White House Officials

Gordon Gray and Andrew Goodpaster—the two members of President Eisenhower's staff who were responsible for national security affairs—both testified that they had no knowledge of any Presidential consideration of assassination during their tenure.[81]

---

[78] See Section 3, *supra,* for discussion of CIA cable traffic indicating that Lumumba continued to be regarded as capable of taking over the government after he was deposed and that pressure to "eliminate" him did not cease until his death.

[79] Bissell was not present at the NSC meeting. (NSC Minutes, 9/21/60)

[80] John Eisenhower, the President's son, who attended the NSC meeting as Assistant White House Staff Secretary, said that he had no "direct recollection" of the discussion but he found the minutes of the meeting consonant with his "recollection of the atmosphere" at the time: "The U.S. position was very much anti-Lumumba." He said:

"I would not conjecture that the words 'disposed of' meant an assassination, if for no other reason than if I had something as nasty as this to plot, I wouldn't do it in front of 21 people * * * the number present [at] the meeting." (Eisenhower, 7/18/75, pp. 9–10)

[81] For a more detailed treatment of the testimony of Gray, Goodpaster, and other Eisenbower Administration officials on the general question of discussion of assassination by the President, see Part 3, Section B(3) (a), *infra.*

Gray served as Special Assistant to the President for National Security Affairs, in which capacity he coordinated the National Security Council and represented the President at Special Group meetings. Gray testified that despite the prevalent attitude of hostility toward Lumumba in the Administration, he did not recall President Eisenhower "ever saying anything that contemplated killing Lumumba." (Gray, 7/9/75, p. 28)[82] When asked to interpret phrases such as "getting rid of" or "disposing of" Lumumba from the minutes of particular NSC and Special Group Meetings, Gray stated:

> It is the intent of the user of the expression or the phrase that is controlling and there may well have been in the Central Intelligence Agency plans and/or discussions of assassinations, but * * * at the level of the Forty Committee [Special Group] or a higher level than that, the National Security Council, there was no active discussion in any way planning assassination.
>
> * * * I agree that assassination could have been on the minds of some people when they used these words 'eliminate' or 'get rid of' * * * I am just trying to say it was not seriously considered as a program of action by the President or even the Forty [Special] Group. (Gray, 7/9/75, pp. 16–17)

Goodpaster, the White House Staff Secretary to President Eisenhower, said that he and Gray were the "principal channels" between the President and the CIA, outside of NSC meetings. Goodpaster was responsible for "handling with the President all matters of day-to-day operations in the general fields of international affairs and security affairs." He regularly attended NSC meetings and was listed among the participants at the NSC meetings of August 18, 1960 and September 21, 1960. (Goodpaster, 7/17/75, pp. 3, 4)

When asked if he ever heard about any assassination effort during the Eisenhower Administration, Goodpaster replied unequivocally:

> * * * at no time and in no way did I ever know of or hear about any mention of such an activity. * * * [I]t is my belief that had such a thing been raised with the President other than in my presence, I would have known about it, and * * * it would have been a matter of such significance and sensitivity that I am confident that * * * I would have recalled it had such a thing happened. (Goodpaster, 7/17/75, p. 5)

John Eisenhower, the President's son who served under Goodpaster as Assistant White House Staff Secretary, stated that the use of assassination was contrary to the President's philosophy that "no man is indispensable." As a participant at NSC meetings who frequently attended Oval Office discussions relating to national security affairs, John Eisenhower testified that nothing that came to his attention in his experience at the White House "can be construed in my mind in the remotest way to mean any Presidential knowledge of our concurrence in any assassination plots or plans." (Eisenhower, 7/18/75, pp. 4, 14)

Each of the other Eisenhower Administration officials who was active in the Special Group in late 1960—Assistant Secretary of Defense John N. Irwin II, Undersecretary of State for Political Affairs Livingston Merchant, and Deputy Secretary of Defense James

[82] At the outset of his testimony on the subject, Gordon Gray acknowledged that he did not have a clear, independent recollection of Lumumba's role in the Congo. (Gray, 7/9/75, pp. 25–26)

Douglas—stated that he did not recall any discussion about assassinating Lumumba. (Irwin affidavit, 9/22/75; Merchant affidavit, 9/8/75; Douglas affidavit, 9/5/75)[83]

Even if the documentary record is read to indicate that there was consideration of assassination at high-level policy meetings, there is no evidence that any officials of the Eisenhower Administration outside the CIA were aware of the specific operational details of the plot to poison Lumumba.[84]

(c) Bissell's Assumptions About Authorization by President Eisenhower and Allen Dulles

Richard Bissell's testimony on the question of high-level authorization for the effort to assassinate Lumumba is problematic. Bissell stated that he had no direct recollection of receiving such authorization and that all of his testimony on this subject "has to be described as inference." (Bissell, 9/10/75, p. 48)

Bissell began his testimony on the subject by asserting that on his own initiative he instructed Michael Mulroney to plan the assassination of Lumumba. (Bissell, 6/11/75, pp. 54–55)[85] Nevertheless, Bissell's conclusion—based on his inferences from the totality of circumstances relating to the entire assassination effort against Lumumba—was that an assassination attempt had been authorized at the highest levels of the government. (Bissell, 9/10/75, pp. 32–33, 47–49, 60–62, 65)

As discussed above, Bissell testified that the minutes of meetings of the Special Group on August 25, 1960 and the NSC on September 21, 1960 indicate that assassination was contemplated at the Presidential level as one acceptable means of "getting rid of Lumumba."[86]

There was "no question," according to Bissell, that the cable from Allen Dulles to the Station Officer in Leopoldville on August 26—which called for Lumumba's "removal" and authorized Hedgman to take action without consulting Headquarters if time did not

[83] Douglas Dillon testified that the subject of assassination never arose in his "direct dealings with either President Eisenhower or President Kennedy." (Dillon, 9/2/75, p. 22) He was asked by a member of the Committee, however, to speculate upon the general philosophical approach that Presidents Eisenhower and Kennedy would have taken to decision-making on the question of using assassination as a tool of foreign policy:

"SENATOR HART (Colorado): I would invite your speculation at this point as a sub-Cabinet officer under President Eisenhower, and as a Cabinet Officer under President Kennedy, I think the Committee would be interested in your view as to the attitude of each of them toward this subject, that is to say, the elimination, violent elimination of foreign leaders.

"DILLON: Well, that is a difficult thing to speculate on in a totally different atmosphere. But I think probably both of them would have approached it in a very pragmatic way, most likely, simply weighed the process and consequence rather than in a way that was primarily of a moral principle. That is what would probably have been their attitude in a few cases. Certainly the idea that this was going to be a policy of the U.S., generally both of them were very much opposed to it." (Dillon, 9/2/75, pp. 22–23)

Dillon served as Undersecretary of State in the Eisenhower Administration and as Secretary of the Treasury under Kennedy.

[84] Although several CIA officers involved in the PROP operation to poison Lumumba testified that the operation was within the scope of actions authorized by the NSC and Special Group, there is no testimony that any official of the Eisenhower Administration outside the CIA had specific knowledge of the operational planning and progress.

[85] See Sections 5 (a) (i) and 5 (a) (ii), *supra.*

[86] See Sections 7 (a) (iii) and 7 (a) (v).

permit—was a direct outgrowth of the Special Group meeting Dulles had attended the previous day. (Bissell, 9/10/75, pp. 31–32) Bissell was "almost certain" that he had been informed about the Dulles cable shortly after its transmission. (Bissell, 9/10/75, p. 12) Bissell said that he assumed that assassination was one of the means of removing Lumumba from the scene that was contemplated by Dulles' cable, despite the fact that it was not explicitly mentioned. (Bissell, 9/10/75, p. 32)

> It is my belief on the basis of the cable drafted by Allen Dulles that he regarded the action of the Special Group as authorizing implementation [of an assassination] if favorable circumstances presented themselves, if it could be done covertly. (Bissell, 9/10/75, pp. 64–65)[87]

Dulles' cable signaled to Bissell that there was Presidential authorization for him to order action to assassinate Lumumba. (Bissell, 9/10/75, pp. 61–62):

Q: Did Mr. Dulles tell you that President Eisenhower wanted Lumumba killed?

Mr. BISSELL: I am sure he didn't.

Q: Did he ever tell you even circumlocutiously through this kind of cable?

Mr. BISSELL: Yes, I think his cable says it in effect. (Bissell, 9/10/75, p. 33)

As for discussions with Dulles about the source of authorization for an assassination effort against Lumumba, Bissell stated:

> I think it is probably unlikely that Allen Dulles would have said either the President or President Eisenhower even to me. I think he would have said, this is authorized in the highest quarters, and I would have known what he meant. (Bissell, 9/10/75, p. 48)

When asked if he had sufficient authority to move beyond the consideration or planning of assassination to order implementation of a plan, Bissell said, "I probably did think I had [such] authority." (Bissell, 9/10/75, pp. 61–62)

When informed of the Station Officer's testimony about the instructions he received from Scheider, Bissell said that despite his absence of a specific recollection:

> I would strongly infer in this case that such an authorization did pass through me, as it were, if Joe Scheider gave that firm instruction to the Station Officer. (Bissell, 9/10/75, p. 40)[88]

Bissell said that the DCI would have been the source of this authorization. (Bissell, 9/10/75, p. 40)

Bissell did not recall being informed by Scheider that Scheider had represented to the Station Officer that Lumumba's assassination had been authorized by the President. But he said that assuming he had instructed Scheider to carry poison to the Congo, "there was no possibility" that he would have issued such an instruction without authorization from

---

[87] Joseph Scheider also testified that, in the context of the Dulles cable, "removal" would signify to someone familiar with "intelligence terminology" a "range of things, from just getting him out of office to killing him." (Scheider, 10/9/75, pp. 45–48)

[88] See Section 7 (d), *infra*, for Scheider's testimony on his impression that Bissell had authorized his assignment to the Congo.

Dulles. Likewise Bissell said he "probably did" tell Scheider that the mission had the approval of President Eisenhower. (Bissell, 9/10/75, pp. 46, 47) This led to Bissell's conclusion that if, in fact, the testimony of the Station Officer about Scheider's actions was accurate, then Scheider's actions were fully authorized.[89] Bissell further stated:

> Knowing Mr. Scheider, it is literally inconceivable to me that we would have acted beyond his instructions. (Bissell, 9/10/75, p. 41)

Bronson Tweedy functioned as a conduit between Bissell and Scheider for instructions relating to the PROP operation. Scheider's impression about the extent of authorization for the assassination operation stemmed ultimately from his conversation with Bissell which was referred to by Tweedy during the meeting in which Scheider was ordered to the Congo.[90]

Tweedy testified that Bissell never referred to the President as the source of authorization for the assassination operation. Tweedy said, however, that the "impression" he derived from his meetings with Bissell and from the Dulles cable of August 26 was that the Agency had authorization at the highest level of the government. But Tweedy found it "very difficult ∗∗∗ to judge whether the President*per se*had been in contact with the Agency" because he was not involved in decisionmaking at "the policy level." (Tweedy, 10/9/75 I, pp. 9, 10)

Concerning the assignment of Mulroney to "plan and prepare for" the assassination of Lumumba, Bissell testified that "it was my own idea to give Mulroney this assignment." But he said that this assignment was made only after an assassination mission against Lumumba already had authorization above the level of DDP. (Bissell, 9/10/75, pp. 24, 50; see also pp. 32–33, 47–48, 60–62)

(d) The Impression of Scheider and Hedgman That the Assassination Operation had Presidential Authorization

The Station Officer and Scheider shared the impression that the President authorized an assassination effort against Lumumba.[91] This impression was derived solely from conversations Scheider had with Bissell and Tweedy. Thus, the testimony of Scheider and the Station Officer does not, in itself, establish Presidential authorization. Neither Scheider nor the Station Officer had first-hand knowledge of any statements by Allen Dulles about Presidential authorization—statements which Bissell assumed he had heard, although he had no specific recollection. Moreover, Scheider may have misconstrued Bissell's reference to "highest authority."

Station Officer Hedgman testified that Scheider indicated to him that President Eisenhower had authorized the assassination of Lumumba by an order to Dulles. Hedgman stated that Scheider initially conveyed this account of Presidential authorization when

---

[89] Q: in light of the entire atmosphere at the Agency and the policy at the Agency at the time Mr. Scheider's representation to the Station Officer that the President bad instructed the DCI to carry out this mission would not have been beyond the pale of Mr. Scheider's authority, at that point?

BISSELL. No, it would not. (Bissell, 9/10/75, p. 65)

[90] See Section 7 (d), *infra*.

[91] See Section 4 (f), *infra*, for additional testimony of the Station Officer and Scheider on this issue.

Hedgman asked him about the source of authority for the Lumumba assassination assignment. (Hedgman, 8/21/75, pp. 30–34)
Hedgman was under the clear impression that the President was the ultimate source of the assassination operation:

Q: Your understanding then was that these instructions were instructions coming to you from the office of the President?

HEDGMAN: That's correct.

Q: Or that he had instructed the Agency, and they were passed on to you?

HEDGMAN: That's right.

Q: You are not the least unclear whether ∗∗∗ the President's name had been invoked in some fashion?

HEDGMAN: At the time, I certainly felt that I was under instructions from the President, yes. (Hedgman, 8/21/75, pp. 32–33)

Hedgman cautioned:

> [A]fter fifteen years, I cannot be 100 percent certain, but I have always, since that date, had the impression in my mind that these orders had come from the President. (Hedgman, 8/21/75, p. 34; *accord,* p. 102)

Hedgman testified that he was under the impression that a "policy decision" had been made—that assassination had been "approved" as "one means" of eliminating Lumumba as a political threat (Hedgman 8/21/75, p. 52):

> I thought the policy decision had been made in the White House, not in the Agency, and that the Agency had been selected as the Executive agent if you will, to carry out a political decision. (Hedgman, 8/21/75, p. 52.)

Although Hedgman assumed that the President had not personally selected the means of assassination, he testified that he was under the impression that the President had authorized the CIA to proceed to take action:

HEDGMAN: ∗∗∗ I doubt that I thought the President had said, you use this system. But my understanding is the President had made a decision that an act should take place, but then put that into the hands of the Agency to carry out his decision.

Q: Whatever that act was to be, it was clearly to be assassination or the death of the foreign political leader?

HEDGMAN: Yes. (Hedgman, 8/21/75, p. 104)

The Station Officer's impression about Presidential authorization stemmed from his conversations with Scheider in the Congo and from his reading of the cable traffic from CIA Headquarters which, in fact, never explicitly mentioned the President although it referred to "high quarters."[92]

[92] See Section 7 (c) for Bissell's interpretation of the reference to "high quarters" in the Dulles cable of August 26, 1960.

Joseph Scheider's testimony about these discussions is compatible with Hedgman's account. (Scheider, 10/7/75, pp. 107–108) Despite the fact that he did not recall mentioning the President by name to Hedgman, Scheider believed that he left Hedgman with the impression that there was Presidential authorization for an assassination attempt against Lumumba. (Scheider, 10/7/75, pp. 103–104, 110; 10/9/75, p. 17) However, Scheider made it clear that the basis for his own knowledge about Presidential authorization for the assassination of Lumumba were the statements to him by Bissell, Tweedy, and Tweedy's Deputy. (Scheider, 10/9/75, pp. 10;/7/75, p. 90)

Scheider testified that in the late summer or early fall of 1960, Richard Bissell asked him to make all the preparations necessary for toxic materials to be ready on short notice for use in the assassination of an unspecified African leader, "in case the decision was to go ahead."[93] (Scheider, 10/7/75, pp. 51–55; 10/9/75, p. 8) Scheider had a specific recollection that Bissell told him that "he had direction from the highest authority" for undertaking an assassination operation. (Scheider, 10/7/75, pp. 51–52, 58):

SCHEIDER: The memory I carry was that he indicated that he had the highest authority for getting into that kind of an operation.

Q: Getting into an operation which would result in the death or incapacitation of a foreign leader?

SCHEIDER: Yes, yes, yes. (Scheider, 10/7/75, p. 52)

Scheider acknowledged the possibility that he "may have been wrong" in his assumptions of Presidential authorization which he based on Bissell's words:

> The specific words, as best I can recollect them, [were] "on the highest authority." (Scheider, 10/9/75, p. 11).

Scheider testified that there was a basis of experience for his assumption that "highest authority" signified the President. He said he "had heard it before" at the CIA and had always interpreted it to denote the President. (Scheider, 10/9/75, p. 51) Likewise, Bronson Tweedy testified that " 'highest authority' was a term that we used in the Agency and it was generally recognized as meaning 'the President'." (Tweedy, 10/9/75 II, p. 20)

According to Scheider, Allen Dulles would have approved the assassination operation before Bissell broached the subject with other CIA officers:

> I would have assumed that Bissell would never have told me that it was to be undertaken under the highest authority until his line ran through Dulles and until Dulles was in on it. (Scheider, 10/7/75, p. 76)

Scheider said that he left the meeting with Bissell under the impression that the Presidential authorization extended only to making preparations to carry out an assassination mission and that the implementation of such a plan might require a separate "go ahead." (Scheider, 10/7/75, pp. 53, 56–8) As far as Scheider was concerned, the "go ahead" on the assassination operation was given to him shortly thereafter by Tweedy and

[93] See section 4 (b), *infra,* for a full treatment of Scheider's meetings with Bissell and his preparation of toxic biological materials and medical paraphernalia pursuant to Bissell's directive.

his Deputy.[94] When they instructed him on his Congo trip, Scheider said Tweedy and his Deputy "referred to the previous conversation I had with Bissell" and they conveyed to Scheider the impression that Bissell "felt the operation had Presidential authority." (Scheider, 10/7/75, pp. 65, 69, 71; 10/9/75, p. 13)[95] Scheider interpreted the statements by Tweedy and his Deputy to mean that Bissell's reference to "highest authority" for the operation had carried over from planning to the implementation stage. (Scheider, 10/7/75, p. 90)

Scheider's impression that there was Presidential authorization for the assassination operation clearly had a powerful influence on the Station Officer's attitude toward undertaking such an assignment.

Hedgman had severe doubts about the wisdom of a policy of assassination in the Congo. At the conclusion of his testimony about the assassination plot, he was asked to give a general characterization of the advisability of the plot and the tenor of the times in which it took place. His response indicated that although he was willing to carry out what he considered a duly authorized order, he was not convinced of the necessity of assassinating Lumumba:

> I looked upon the Agency as an executive arm of the Presidency * * *. Therefore, I suppose I thought that it was an order issued in due form from an authorized authority.
>
> On the other hand, I looked at it as a kind of operation that I could do without, that I thought that probably the Agency and the U.S. government could get along without. I didn't regard Lumumba as the kind of person who was going to bring on World War III.
>
> I might have had a somewhat different attitude if I thought that one man could bring on World War III and result in the deaths of millions of people or something, but I didn't see him in that light. I saw his as a danger to the political position of the United States in Africa, but nothing more than that. (Hedgman, 8/21/75, pp. 110–111)

[94] See Section 4 (c), *infra*, for a detailed account of the testimony about the meeting of Tweedy, his Deputy, and Scheider.

[95] Tweedy was unable to shed much light on the discussion of authorization at his meeting with Scheider:

I do not recall that Scheider and I ever discussed higher authority and approval. I do not say that it did not occur." (Tweedy, 10/9/75, p. 65)

APPENDIX G

THE EXECUTIVE ORDER PROHIBITING ASSASSINATION PLOTS, 1976

PRESIDENT GERALD R. FORD'S EXECUTIVE ORDER 11905: UNITED STATES FOREIGN INTELLIGENCE ACTIVITIES

February 18, 1976

. . . . *(g) Prohibition of Assassination.* No employee of the United States Government shall engage in, or conspire to engage in, political assassination. . . .

Source: *Weekly Compilation of Presidential Documents*, vol. 12 (February 23, 1976), p. 15.

APPENDIX H

WHEN COVERT ACTION SUBVERTS U.S. LAW: THE IRAN-*CONTRA* CASE

Tower Commission

In the aftermath of the Iran-*contra* scandal involving questionable arms sales to Iran and the funneling of the profits to the *contras* for a covert war in Nicaragua, President Ronald Reagan established a blue-ribbon panel to investigate the affair. The president selected a former U.S. senator, Republican John Tower of Texas, to head up the inquiry. This selection summarizes the commission's findings, which were highly critical of both the president and the NSC staff.

WHAT WAS WRONG

The arms transfers to Iran and the activities of the NSC staff in support of the Contras are case studies in the perils of policy pursued outside the constraints of orderly process.

The Iran initiative ran directly counter to the Administration's own policies on terrorism, the Iran/Iraq war, and military support to Iran. This inconsistency was never re-

Sources: Report of the President's *Special Review Board* (Tower Commission), Washington, DC, February 26, 1987), pp. IV, 1–13; and witness testimony, *Hearings,* Select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition (the Inouye-Hamilton Joint Committee, co-chaired by Senator Daniel K. Inouye, D-Hawaii, and Representative Lee Hamilton, D-Indiana), July and August 1987. The Tower Commission members included the chair, John Tower (R-Texas); Edmund Muskie, former Democratic Senator from Maine and secretary of state in the Carter administration; and Brent Scowcroft, national security adviser in the Ford and first Bush administrations. In the second part of this appendix, the congressional testimony is from national security adviser Vice Admiral John M. Poindexter and NSC staff aide Lieut. Col. Oliver L. North, as well as Secretary of State George P. Shultz.

solved, nor were the consequences of this inconsistency fully considered and provided for. The result taken as a whole was a U.S. policy that worked against itself.

The Board believes that failure to deal adequately with these contradictions resulted in large part from the flaws in the manner in which decisions were made. Established procedures for making national security decisions were ignored. Reviews of the initiative by all the NSC principals were too infrequent. The initiatives were not adequately vetted below the cabinet level. Intelligence resources were underutilized. Applicable legal constraints were not adequately addressed. The whole matter was handled too informally, without adequate written records of what had been considered, discussed, and decided.

This pattern persisted in the implementation of the Iran initiative. The NSC staff assumed direct operational control. The initiative fell within the traditional jurisdictions of the Departments of State, Defense, and CIA. Yet these agencies were largely ignored. Great reliance was placed on a network of private operators and intermediaries. How the initiative was to be carried out never received adequate attention from the NSC principals or a tough working-level review. No periodic evaluation of the progress of the initiative was ever conducted. The result was an unprofessional and, in substantial part, unsatisfactory operation.

In all of this process, Congress was never notified. . . .

A. A FLAWED PROCESS

1. Contradictory Policies Were Pursued

The arms sales to Iran and the NSC support for the Contras demonstrate the risks involved when highly controversial initiatives are pursued covertly.

ARMS TRANSFERS TO IRAN

The initiative to Iran was a covert operation directly at odds with important and well-publicized policies of the Executive Branch. But the initiative itself embodied a fundamental contradiction. Two objectives were apparent from the outset: a strategic opening to Iran, and release of the U.S. citizens held hostage in Lebanon. The sale of arms to Iran appeared to provide a means to achieve both these objectives. It also played into the hands of those who had other interests—some of them personal financial gain—in engaging the United States in an arms deal with Iran.

In fact, the sale of arms was not equally appropriate for achieving both these objectives. Arms were what Iran wanted. If all the United States sought was to free the hostages, then an arms-for-hostages deal could achieve the immediate objectives of both sides. But if the U.S. objective was a broader strategic relationship, then the sale of arms should have been contingent upon first putting into place the elements of that relationship. An arms-for-hostages deal in this context could become counter-productive to achieving this broader strategic objective. In addition, release of the hostages would require exerting influence with Hizballah, which could involve the most radical elements of the Iranian regime. The kind of strategic opening sought by the United States, however, involved what were regarded as more moderate elements.

The U.S. officials involved in the initiative appeared to have held three distinct views. For some, the principal motivation seemed consistently a strategic opening to Iran. For others, the strategic opening became a rationale for using arms sales to obtain the release of

the hostages. For still others, the initiative appeared clearly as an arms-for-hostages deal from first to last.

Whatever the intent, almost from the beginning the initiative became in fact a series of arms-for-hostages deals. . . .

While the United States was seeking the release of the hostages in this way, it was vigorously pursuing policies that were dramatically opposed to such efforts. The Reagan Administration in particular had come into office declaring a firm stand against terrorism, which it continued to maintain. In December of 1985, the Administration completed a major study under the chairmanship of the Vice President. It resulted in a vigorous reaffirmation of U.S. opposition to terrorism in all its forms and a vow of total war on terrorism whatever its source. The Administration continued to pressure U.S. allies not to sell arms to Iran and not to make concessions to terrorists.

No serious effort was made to reconcile the inconsistency between these policies and the Iran initiative. No effort was made systematically to address the consequences of this inconsistency—the effect on U.S. policy when, as it inevitably would, the Iran initiative became known. . . .

NSC STAFF SUPPORT FOR THE CONTRAS

The activities of the NSC staff in support of the Contras sought to achieve an important objective of the Administration's foreign policy. The President had publicly and emphatically declared his support for the Nicaragua resistance. That brought his policy in direct conflict with that of the Congress, at least during the period that direct or indirect support of military operations in Nicaragua was barred.

Although the evidence before the Board is limited, no serious effort appears to have been made to come to grips with the risks to the President of direct NSC support for the Contras in the face of these Congressional restrictions. Even if it could be argued that these restrictions did not technically apply to the NSC staff, these activities presented great political risk to the President. The appearance of the President's personal staff doing what Congress had forbade other agencies to do could, once disclosed, only touch off a firestorm in the Congress and threaten the Administration's whole policy on the Contras.

2. The Decision-making Process Was Flawed

Because the arms sales to Iran and the NSC support for the Contras occurred in settings of such controversy, one would expect that the decisions to undertake these activities would have been made only after intense and thorough consideration. In fact, a far different picture emerges.

ARMS TRANSFERS TO IRAN

The Iran initiative was handled almost casually and through informal channels, always apparently with an expectation that the process would end with the next arms-for-hostages exchange. It was subjected neither to the general procedures for interagency consideration and review of policy issues nor the more restrictive procedures set out in NSDD 159 for handling covert operations. This had a number of consequences.

(i) The opportunity for a full hearing before the President was inadequate. In the last half of 1985, the Israelis made three separate proposals to the United States with respect to

the Iran initiative (two in July and one in August). In addition, Israel made three separate deliveries of arms to Iran, one each in August, September, and November. Yet prior to December 7, 1985, there was at most one meeting of the NSC principals, a meeting which several participants recall taking place on August 6. There is no dispute that full meetings of the principals did occur on December 7, 1985, and on January 7, 1986. But the proposal to shift to direct U.S. arms sales to Iran appears not to have been discussed until later. It was considered by the President at a meeting on January 17 which only the Vice President, Mr. Regan, Mr. Fortier, and VADM Poindexter attended. Thereafter, the only senior-level review the Iran initiative received was during one or another of the President's daily national security briefings. These were routinely attended only by the President, the Vice President, Mr. Regan, and VADM Poindexter. There was no subsequent collective consideration of the Iran initiative by the NSC principals before it became public 11 months later.

This was not sufficient for a matter as important and consequential as the Iran initiative. Two or three cabinet-level reviews in a period of 17 months was not enough. The meeting on December 7 came late in the day, after the pattern of arms-for-hostages exchanges had become well established. The January 7 meeting had earmarks of a meeting held after a decision had already been made. Indeed, a draft Covert Action Finding authorizing the initiative had been signed by the President, though perhaps inadvertently, the previous day.

At each significant step in the Iran initiative, deliberations among the NSC principals in the presence of the President should have been virtually automatic. This was not and should not have been a formal requirement, something prescribed by statute. Rather, it should have been something the NSC principals desired as a means of ensuring an optimal environment for Presidential judgment. The meetings should have been preceded by consideration by the NSC principals of staff papers prepared according to the procedures applicable to covert actions. These should have reviewed the history of the initiative, analyzed the issues then presented, developed a range of realistic options, presented the odds of success and the costs of failure, and addressed questions of implementation and execution. Had this been done, the objectives of the Iran initiative might have been clarified and alternatives to the sale of arms might have been identified.

(ii) The initiative was never subjected to a rigorous review below the cabinet level. Because of the obsession with secrecy, interagency consideration of the initiative was limited to the cabinet level. With the exception of the NSC staff and, after January 17, 1986, a handful of CIA officials, the rest of the executive departments and agencies were largely excluded.

As a consequence, the initiative was never vetted at the staff level. This deprived those responsible for the initiative of considerable expertise—on the situation in Iran; on the difficulties of dealing with terrorists; on the mechanics of conducting a diplomatic opening. It also kept the plan from receiving a tough, critical review.

Moreover, the initiative did not receive a policy review below cabinet level. Careful consideration at the Deputy/Under Secretary level might have exposed the confusion in U.S. objectives and clarified the risks of using arms as an instrument of policy in this instance.

The vetting process would also have ensured better use of U.S. intelligence. As it was, the intelligence input into the decision process was clearly inadequate. First, no independent evaluation of other Israeli proposals offered in July and August appears to have

been sought or offered by U.S. intelligence agencies. The Israelis represented that they for some time had had contacts with elements in Iran. The prospects for an opening to Iran depended heavily on these contacts, yet no systematic assessment appears to have been made by U.S. intelligence agencies of the reliability and motivations of these contacts, and the identity and objectives of the elements in Iran that the opening was supposed to reach. Neither was any systematic assessment made of the motivation of the Israelis.

Second, neither Mr. Ghorbanifar nor the second channel seem to have been subjected to a systematic intelligence vetting before they were engaged as intermediaries. Mr. Ghorbanifar had been known to the CIA for some time and the agency had substantial doubts as to his reliability and truthfulness. Yet the agency did not volunteer that information or inquire about the identity of the intermediary if his name was unknown. Conversely, no early request for a name check was made of the CIA, and it was not until January 11, 1986, that the agency gave Mr. Ghorbanifar a new polygraph, which he failed. Notwithstanding this situation, with the signing of the January 17 Finding, the United States took control of the initiative and became even more directly involved with Mr. Ghorbanifar. The issues raised by the polygraph results do not appear to have been systematically addressed. In similar fashion, no prior intelligence check appears to have been made on the second channel.

Third, although the President recalled being assured that the arms sales to Iran would not alter the military balance with Iran, the Board could find no evidence that the President was ever briefed on this subject. The question of the impact of any intelligence shared with the Iranians does not appear to have been brought to the President's attention.

A thorough vetting would have included consideration of the legal implications of the initiative. There appeared to be little effort to face squarely the legal restrictions and notification requirements applicable to the operation. At several points, other agencies raised questions about violations of law or regulations. These concerns were dismissed without, it appears, investigating them with the benefit of legal counsel.

Finally, insufficient attention was given to the implications of implementation. The implementation of the initiative raised a number of issues: should the NSC staff rather than the CIA have had operational control; what were the implications of Israeli involvement; how reliable were the Iranian and various other private intermediaries; what were the implications of the use of Mr. Secord's private network of operatives; what were the implications for the military balance in the region; was operational security adequate. Nowhere do these issues appear to have been sufficiently addressed.

The concern for preserving the secrecy of the initiative provided an excuse for abandoning sound process. Yet the initiative was known to a variety of persons with diverse interests and ambitions—Israelis, Iranians, various arms dealers and business intermediaries, and Lt. Col. North's network of private operatives. While concern for secrecy would have justified limiting the circle of persons knowledgeable about the initiative, in this case it was drawn too tightly. As a consequence, important advice and counsel were lost.

In January of 1985, the President had adopted procedures for striking the proper balance between secrecy and the need for consultation on sensitive programs. These covered the institution, implementation, and review of covert operations. In the case of the Iran initiative, these procedures were almost totally ignored.

The only staff work the President apparently reviewed in connection with the Iran initiative was prepared by NSC staff members, under the direction of the National Security Advisor. These were, of course, the principal proponents of the initiative. A portion of this

staff work was reviewed by the Board. It was frequently striking in its failure to present the record of past efforts—particularly past failures. Alternative ways of achieving U.S. objectives—other than yet another arms-for-hostages deal—were not discussed. Frequently it neither adequately presented the risks involved in pursuing the initiative nor the full force of the dissenting views of other NSC principals. On balance, it did not serve the President well.

(iii) The process was too informal. The whole decision process was too informal. Even when meetings among NSC principals did occur, often there was no prior notice of the agenda. No formal written minutes seem to have been kept. Decisions subsequently taken by the President were not formally recorded. An exception was the January 17 Finding, but even this was apparently not circulated or shown to key U.S. officials.

The effect of this informality was that the initiative lacked a formal institutional record. This precluded the participants from undertaking the more informed analysis and reflection that is afforded by a written record, as opposed to mere recollection. It made it difficult to determine where the initiative stood, and to learn lessons from the record that could guide future action. This lack of an institutional record permitted specific proposals for arms-for-hostages exchanges to be presented in a vacuum, without reference to the results of past proposals. Had a searching and thorough review of the Iran initiative been undertaken at any stage in the process, it would have been extremely difficult to conduct. The Board can attest first hand to the problem of conducting a review in the absence of such records. Indeed, the exposition in the wake of public revelation suffered the most.

NSC STAFF SUPPORT FOR THE CONTRAS

It is not clear how Lt. Col. North first became involved in activities in direct support of the Contras during the period of the Congressional ban. The Board did not have before it much evidence on this point. In the evidence that the Board did have, there is no suggestion at any point of any discussion of Lt. Col. North's activities with the President in any forum. There also does not appear to have been any interagency review of Lt. Col. North's activities at any level.

This latter point is not surprising given the Congressional restrictions under which the other relevant agencies were operating. But the NSC staff apparently did not compensate for the lack of any interagency review with its own internal vetting of these activities. Lt. Col. North apparently worked largely in isolation, keeping first Mr. McFarlane and then VADM Poindexter informed.

The lack of adequate vetting is particularly evident on the question of the legality of Lt. Col. North's activities. The Board did not make a judgment on the legal issues raised by his activities in support of the Contras. Nevertheless, some things can be said.

If these activities were illegal, obviously they should not have been conducted. If there was any doubt on the matter, systematic legal advice should have been obtained. The political cost to the President of illegal action by the NSC staff was particularly high, both because the NSC staff is the personal staff of the President and because of the history of serious conflict with the Congress over the issue of Contra support. For these reasons, the President should have been kept apprised of any review of the legality of Lt. Col. North's activities.

Legal advice was apparently obtained from the President's Intelligence Oversight Board. Without passing on the quality of that advice, it is an odd source. It would be one

thing for the Intelligence Oversight Board to review the legal advice provided by some other agency. It is another for the Intelligence Oversight Board to be originating legal advice of its own. That is a function more appropriate for the NSC staff's own legal counsel.

3. Implementation Was Unprofessional

The manner in which the Iran initiative was implemented and Lt. Col. North undertook to support the Contras are very similar. This is in large part because the same cast of characters was involved. In both cases the operations were unprofessional, although the Board has much less evidence with respect to Lt. Col. North's Contra activities.

ARMS TRANSFERS TO IRAN

With the signing of the January 17 Finding, the Iran initiative became a U.S. operation run by the NSC staff. Lt. Col. North made most of the significant operational decisions. He conducted the operation through Mr. Secord and his associates, a network of private individuals already involved in the Contra resupply operation. To this was added a handful of selected individuals from the CIA.

But the CIA support was limited. Two CIA officials, though often at meetings, had a relatively limited role. One served as the point man for Lt. Col. North in providing logistics and financial arrangements. The other (Mr. Allen) served as a contact between Lt. Col. North and the intelligence community. By contrast, George Cave actually played a significant and expanding role. However, Clair George, Deputy Director for Operations at CIA, told the Board: "George was paid by me and on the paper was working for me. But I think in the heat of the battle, . . . George was working for Oliver North."

Because so few people from the departments and agencies were told of the initiative, Lt. Col. North cut himself off from resources and expertise from within the government. He relied instead on a number of private intermediaries, businessmen and other financial brokers, private operators, and Iranians hostile to the United States. Some of these were individuals with questionable credentials and potentially large personal financial interests in the transactions. This made the transactions unnecessarily complicated and invited kickbacks and payoffs. This arrangement also dramatically increased the risks that the initiative would leak. Yet no provision was made for such an eventuality. Further, the use of Mr. Secord's private network in the Iran initiative linked those operators with the resupply of the Contras, threatening exposure of both operations if either became public.

The result was a very unprofessional operation. . . .

The implementation of the initiative was never subjected to a rigorous review. Lt. Col. North appears to have kept VADM Poindexter fully informed of his activities. In addition, VADM Poindexter, Lt. Col. North, and the CIA officials involved apparently apprised Director Casey of many of the operational details. But Lt. Col. North and his operation functioned largely outside the orbit of the U.S. Government. Their activities were not subject to critical reviews of any kind.

After the initial hostage release in September, 1985, it was over 10 months before another hostage was released. This despite recurring promises of the release of all the hostages and four intervening arms shipments. Beginning with the November shipment, the United States increasingly took over the operation of the initiative. In January, 1986, it decided to transfer arms directly to Iran.

Any of these developments could have served as a useful occasion for a systematic reconsideration of the initiative. Indeed, at least one of the schemes contained a provision for reconsideration if the initial assumptions proved to be invalid. They did, but the reconsideration never took place. It was the responsibility of the National Security Advisor and the responsible officers on the NSC staff to call for such a review. But they were too involved in the initiative both as advocates and as implementors. This made it less likely that they would initiate the kind of review and reconsideration that should have been undertaken.

NSC STAFF SUPPORT FOR THE CONTRAS

As already noted, the NSC activities in support of the Contras and its role in the Iran initiative were of a piece. In the former, there was an added element of Lt. Col. North's intervention in the customs investigation of the crash of the SAT aircraft. Here, too, selected CIA officials reported directly to Lt. Col. North. The limited evidence before the Board suggested that the activities in support of the Contras involved unprofessionalism much like that in the Iran operation.

iv. Congress was never notified. Congress was not apprised either of the Iran initiative or of the NSC staff's activities in support of the Contras.

In the case of Iran, because release of the hostages was expected within a short time after the delivery of equipment, and because public disclosure could have destroyed the operation and perhaps endangered the hostages, it could be argued that it was justifiable to defer notification of Congress prior to the first shipment of arms to Iran. The plan apparently was to inform Congress immediately after the hostages were safely in U.S. hands. But after the first delivery failed to release all the hostages, and as one hostage release plan was replaced by another, Congress certainly should have been informed. This could have been done during a period when no specific hostage release plan was in execution, Consultation with Congress could have been useful to the President, for it might have given him some sense of how the public would react to the initiative. It also might have influenced his decision to continue to pursue it. . . .

B. FAILURE OF RESPONSIBILITY

The NSC system will not work unless the President makes it work. After all, this system was created to serve the President of the United States in ways of his choosing. By his actions, by his leadership, the President therefore determines the quality of its performance.

By his own account, as evidenced in his diary notes, and as conveyed to the Board by his principal advisors, President Reagan was deeply committed to securing the release of the hostages. It was this intense compassion for the hostages that appeared to motivate his steadfast support of the Iran initiative, even in the face of opposition from his Secretaries of State and Defense.

In his obvious commitment, the President appears to have proceeded with a concept of the initiative that was not accurately reflected in the reality of the operation. The President did not seem to be aware of the way in which the operation was implemented and the full consequences of U.S. participation.

The President's expressed concern for the safety of both the hostages and the Iranians who could have been at risk may have been conveyed in a manner so as to inhibit the full functioning of the system.

The President's management style is to put the principal responsibility for policy review and implementation on the shoulders of his advisors. Nevertheless, with such a complex, high-risk operation and so much at stake, the President should have ensured that the NSC system did not fail him. He did not force his policy to undergo the most critical review of which the NSC participants and the process were capable. At no time did he insist upon accountability and performance review. Had the President chosen to drive the NSC system, the outcome could well have been different. As it was, the most powerful features of the NSC system—providing comprehensive analysis, alternatives and follow-up—were not utilized.

The Board found a strong consensus among NSC participants that the President's priority in the Iran initiative was the release of U.S. hostages. But setting priorities is not enough when it comes to sensitive and risky initiatives that directly affect U.S. national security. He must ensure that the content and tactics of an initiative match his priorities and objectives. He must insist upon accountability. For it is the President who must take responsibility for the NSC system and deal with the consequences.

Beyond the President, the other NSC principals and the National Security Advisor must share in the responsibility for the NSC system.

President Reagan's personal management style places an especially heavy responsibility on his key advisors. Knowing his style, they should have been particularly mindful of the need for special attention to the manner in which this arms sale initiative developed and proceeded. On this score, neither the National Security Advisor nor the other NSC principals deserve high marks.

It is their obligation as members and advisors to the Council to ensure that the President is adequately served. The principal subordinates to the President must not be deterred from urging the President not to proceed on a highly questionable course of action even in the face of his strong conviction to the contrary.

In the case of the Iran initiative, the NSC process did not fail, it simply was largely ignored. The National Security Advisor and the NSC principals all had a duty to raise this issue and insist that orderly process be imposed. None of them did so.

All had the opportunity. While the National Security Advisor had the responsibility to see that an orderly process was observed, his failure to do so does not excuse the other NSC principals. It does not appear that any of the NSC principals called for more frequent consideration of the Iran initiative by the NSC principals in the presence of the President. None of the principals called for a serious vetting of the initiative by even a restricted group of disinterested individuals. The intelligence questions do not appear to have been raised, and legal considerations, while raised, were not pressed. No one seemed to have complained about the informality of the process. No one called for a thorough reexamination once the initiative did not meet expectations or the manner of execution changed. While one or another of the NSC principals suspected that something was amiss, none vigorously pursued the issue.

Mr. Regan also shares in this responsibility. More than almost any Chief of Staff of recent memory, he asserted personal control over the White House staff and sought to extend this control to the National Security Advisor. He was personally active in national security affairs and attended almost all of the relevant meetings regarding the Iran initiative.

He, as much as anyone, should have insisted that an orderly process be observed. In addition, he especially should have ensured that plans were made for handling any public disclosure of the initiative. He must bear primary responsibility for the chaos that descended upon the White House when such disclosure did occur.

Mr. McFarlane appeared caught between a President who supported the initiative and the cabinet officers who strongly opposed it. While he made efforts to keep these cabinet officers informed, the Board heard complaints from some that he was not always successful. VADM Poindexter on several occasions apparently sought to exclude NSC principals other than the President from knowledge of the initiative. Indeed, on one or more occasions Secretary Shultz may have been actively misled by VADM Poindexter.

VADM Poindexter also failed grievously on the matter of Contra diversion. Evidence indicates that VADM Poindexter knew that a diversion occurred, yet he did not take the steps that were required given the gravity of that prospect. He apparently failed to appreciate or ignored the serious legal and political risks presented. His clear obligation was either to investigate the matter or take it to the President—or both. He did neither. Director Casey shared a similar responsibility. Evidence suggests that he received information about the possible diversion of funds to the Contras almost a month before the story broke. He, too, did not move promptly to raise the matter with the President. Yet his responsibility to do so was clear.

The NSC principals other than the President may be somewhat excused by the insufficient attention on the part of the National Security Advisor to the need to keep all the principals fully informed. Given the importance of the issue and the sharp policy divergences involved, however, Secretary Shultz and Secretary Weinberger in particular distanced themselves from the march of events. Secretary Shultz specifically requested to be informed only as necessary to perform his job. Secretary Weinberger had access through intelligence to details about the operation. Their obligation was to give the President their full support and continued advice with respect to the program or, if they could not in conscience do that, to so inform the President. Instead, they simply distanced themselves from the program. They protected the record as to their own positions on this issue. They were not energetic in attempting to protect the President from the consequences of his personal commitment to freeing the hostages.

Director Casey appears to have been informed in considerable detail about the specifics of the Iranian operation. He appears to have acquiesced in and to have encouraged North's exercise of direct operational control over the operation. Because of the NSC staff's proximity to and close identification with the President, this increased the risks to the President if the initiative became public or the operation failed.

There is no evidence, however, that Director Casey explained this risk to the President or made clear to the President that Lt. Col. North, rather than the CIA, was running the operation. The President does not recall ever being informed of this fact. Indeed, Director Casey should have gone further and pressed for operational responsibility to be transferred to the CIA.

Director Casey should have taken the lead in vetting the assumptions presented by the Israelis on which the program was based and in pressing for an early examination of the reliance upon Mr. Ghorbanifar and the second channel as intermediaries. He should also have assumed responsibility for checking out the other intermediaries involved in the operation. Finally, because Congressional restrictions on covert actions are both largely

directed at and familiar to the CIA, Director Casey should have taken the lead in keeping the question of Congressional notification active.

Finally, Director Casey, and, to a lesser extent, Secretary Weinberger, should have taken it upon themselves to assess the effect of the transfer of arms and intelligence to Iran on the Iran/Iraq military balance, and to transmit that information to the President. . . .

Inouye—Hamilton Committee

In response to the Iran-*contra* scandal, the Congress created an investigative panel to examine what had happened. The House-Senate Joint Committee heard from twenty-eight witnesses in public hearings, including Lieut. Col. Oliver L. North, Vice Admiral John N. Poindexter (President Reagan's national security adviser at the time), and Secretary of State George P. Shultz. Their testimony, excerpted in this selection, takes us behind the scenes of the Iran-*contra* affair, disclosing many of the intrigues that occurred inside the NSC during this period, as well as the systematic attempts by several key NSC officials to conceal them from lawmakers.

THE COMMITTEE HEARD FROM LIEUT. COL. OLIVER L. NORTH IN JULY OF 1987

JULY 7, 1987

John W. Nields Jr., chief counsel for the House.

Q The American people were told by this Government that our Government had nothing to do with the Hasenfus airplane [a secret CIA military-supply flight which crashed in Nicaragua in 1986], and that was false. And it is a principal purpose of these hearings to replace secrecy and deception with disclosure and truth. And that's one of the reasons we have called you here, sir. And one question the American people would like to know the answer to is what did the President know about the diversion of the proceeds of Iranian arms sales to the contras. Can you tell us what you know about that, sir?

A You just took a long leap from Mr. Hasenfus's airplane.

As I told this committee several days ago—and if you will indulge me, counsel, in a brief summary of what I said: I never personally discussed the use of the residuals or profits from the sale of U.S. weapons to Iran for the purpose of supporting the Nicaraguan resistance with the President. I never raised it with him and he never raised it with me during my entire tenure with the National Security Council staff.

Throughout the conduct of my entire tenure at the National Security Council, I assumed that the President was aware of what I was doing and had, through my superiors, approved it. I sought approval of my superiors for every one of my actions, and it is well documented.

I assumed, when I had approval to proceed from either Judge Clark, Bud McFarlane or Admiral Poindexter, that they had indeed solicited and obtained the approval of the President. To my recollection, Admiral Poindexter never told me that he met with the President on the issue of using residuals from the Iranian sales to support the Nicaraguan resistance. Or that he discussed the residuals or profits for use by the contras with the President. Or that he got the President's specific approval.

Nor did he tell me that the President had approved such a transaction.

But again, I wish to reiterate throughout I believed that the President had indeed authorized such activity.

No other person with whom I was in contact with during my tenure at the White House told me that he or she ever discussed the issue of the residuals or profits with the President.

In late November, two other things occurred which relate to this issue. On or about Friday, Nov. 21, [1986] I asked Admiral Poindexter directly: Does the President know? He told me he did not. And on Nov. 25, the day I was reassigned back to the United States Marine Corps for service, the President of the United States called me. In the course of that call, the President said to me words to the effect that: I just didn't know.

Those are the facts as I know them, Mr. Nields. I was glad that . . . you said that you wanted to hear the truth. I came here to tell you the truth, the good, the bad and the ugly. I am here to tell it all, pleasant and unpleasant. And I am here to accept responsibility for that which I did. I will not accept responsibility for that which I did not do. . . .

Q I'm not asking you about words now, Colonel. I am asking you whether you didn't continue to send memoranda seeking approval of diversions or residuals—whatever the word—for the benefit of the contras up to the President for approval?

A I did not send them to the President, Mr. Nields. This memorandum went to the National Security Adviser, seeking that he obtain the President's approval. There is a big difference. This is not a memorandum to the President.

Q And my question to you is: Didn't—isn't it true that you continued to send them up to the National Security Adviser, seeking the President's approval?

A Is it my recollection that I did, yes sir.

Q And Admiral Poindexter never told you: Stop sending those memoranda?

A I do not recall the admiral saying that. It is entirely possible, Mr. Nields, that that did happen.

Q Well if it had happened, then you would have stopped sending them, isn't that true?

A Yes.

Q But you didn't stop sending them. You've just testified you sent them on five different occasions.

A I testified that to my recollection there were about five times when we thought we had an arrangement that would result in the release of American hostages and the opening of a dialogue with Iran. And that we thought the deal was sufficiently framed that we could proceed with it. And that I thought—because I don't have those records before me—that I had sent memoranda forward, as I always did, seeking approval.

That's what I think and that's what I recall.

Q And was there ever a time when Admiral Poindexter said: Don't send them up for the President's approval; just send them up for my approval?

A Again, I don't recall such a conversation.

Q Well in fact, isn't it true that it was Admiral Poindexter that wanted you to send these memoranda up for the President to approve?

A I don't recall Admiral Poindexter instructing me to do that, either. . . .

Q So far from telling you to stop sending memoranda up for the President's approval, Admiral Poindexter was specifically asking you to send memoranda up for the President's approval?

A Well, again, in this particular case that's true, Mr. Nields. And I don't believe that I have said that Admiral Poindexter told me to stop. Did I?

Q Where are these memoranda?

A Which memoranda?

Q The memoranda that you sent up to Admiral Poindexter, seeking the President's approval?

A Well, they're probably in these books to my left that I haven't even looked through yet. And if I try to guess, I'm going to be wrong. But I think I shredded most of that. Did I get them all. I'm not trying to be flippant, I'm just—

Q Well, that was going to be my very next question, Colonel North. Isn't it true that you shredded them?

A I believe I did. . . .

Q Well, that's the whole reason for shredding documents, isn't it, Colonel North—so that you can later say you don't remember whether you had them and you don't remember what's in them?

A No, Mr. Nields. The reason for shredding documents and the reason the Government of the United States gave me a shredder—I mean, I didn't buy it myself—was to destroy documents that were no longer relevant; that did not apply or that should not be divulged.

And again, I want to go back to the whole intent of a covert operation. Part of a covert operation is to offer plausible deniability of the association of the Government of the United States with the activity. Part of it is to deceive our adversaries. Part of it is to insure that those people who are at great peril carrying out those activities are not further endangered.

All of those are good and sufficient reasons to destroy documents. And that's why the Government buys [and] gives them to people running [a] covert operation. Not so that they can have convenient memories. I came here to tell you the truth; to tell you and this committee and the American people the truth. And I'm trying to do that, Mr. Nields. And I don't like the insinuation that I'm up here having a convenient memory lapse like perhaps some others have had. . . .

Q Is it correct to say that following the enactment of the Boland Amendment, our support for the war in Nicaragua did not end and that you were the person in the United States Government who managed it?

A Starting in the spring of 1984, well before the Boland proscription of no appropriated funds made available to the D.O.D. and the C.I.A., etc., I was already engaged in supporting the Nicaraguan resistance and the democratic outcome in Nicaragua.

I did so as part of a covert operation. It was carried out starting as early as the spring of '84, when we ran out of money and people started to look in Nicaragua, in Honduras and Guatemala, El Salvador and Costa Rica for some sign of what the Americans were really going to do, and that that help began much earlier than the most rigorous of the Boland proscriptions. And yes, it was carried out covertly, and it was carried out in such a way as to insure that the heads of state and the political leadership in Nicaragua—in Central America—recognized the United States was going to meet the commitments of the President's foreign policy.

And the President's foreign policy was that we are going to achieve a democratic outcome in Nicaragua and that our support for the Nicaraguan freedom fighters was

going to continue, and that I was given the job of holding them together in body and soul. And it slowly transitioned into a more difficult task as time went on and as the C.I.A. had to withdraw further and further from that support, until finally we got to the point in October when I was the only person left talking to them. . . .

Q Well maybe it would be most useful to get into specifics of the areas of your support. I take it one area of your support was to endeavor to raise money from sources other than the U.S. Treasury?

A That's correct. Boland proscriptions do not allow us to do so, and so we sought a means of complying with those Boland proscriptions by going elsewhere for those monies.

Q And you went to foreign countries?

A I did not physically go to those foreign countries.

Q Representatives of—

A Representatives of foreign countries and I had discussions about those matters, yes.

Q And you asked them for money for the contras?

A I want to be a little bit more specific about that. I don't recall going hat in hand to anybody asking for money. I do recall sitting and talking about how grateful this country would be if the issue that they had discussed with others were indeed brought to fruition. For example, a representative of Country 3 and I met and we talked about an issue that had been raised with him beforehand by others outside the Government, and I told him that I thought that was a dandy idea. And I told him where he could send the money. And he did so. . . .

Q Now, my next question is you've indicated that the national security advisers, for whom you worked, authorized you to seek support from foreign countries, both financial and operational?

A Yes.

Q Was your—were your activities, in that respect, known to others in the White House, other than the national security advisers?

A Well, I want to go back to something I said at the very beginning of all of this, Mr. Nields. I assumed that those matters which required the attention and decision of the President of the United States did indeed get them.

I assumed that. I never asked that. I never walked up to the President and said, oh by the way Mr. President, yesterday I met with so-and-so from Country 4. Nor did he ever say, I'm glad you had a meeting with Country 4 and it went well.

Q Do you know whether or not the President was aware of your activities seeking funds and operational support for the contras, from third countries?

A I do not know.

Q Were you ever—

A I assumed that he did.

Q Were you ev—what was the basis of your assumption?

A Just that there was a lot going on and it was very obvious that the Nicaraguan resistance survived—I sent forward innumerable documents, some of which you've just shown us as exhibits, that demonstrated that I was keeping my superiors fully informed, as to what was going on. . . .

Q Mr. McFarlane has testified that he gave you instructions not to solicit money from foreign countries or private sources. Did he give you those instructions?

A I never carried out a single act—not one, Mr. Nields—in which I did not have authority from my superiors. I haven't, in the 23 years that I have been in the uniformed services of the United States of America ever violated an order—not one.

Q But that wasn't the question. The question was—

A That *is* the answer to your question.

Q No, the question was did Mr. McFarlane give you such instructions?

A No. I never heard those instructions.

Q And I take it that it was your understanding, from what you've just said, that quite to the contrary, you were authorized to seek money from foreign countries?

A I was authorized to do everything that I did.

Q Well, again, that isn't the question.

A I was authorized to have a meeting, in this particular case by Mr. McFarlane, for the purpose of talking to the man about a suggestion that had been made to him by others, and to encourage that process along. And I did so. I had already provided to Mr. McFarlane a card with the address of an account, an offshore account which would support the Nicaraguan resistance. And thank God, somebody put money into that account and the Nicaraguan resistance didn't die—as perhaps others intended. Certainly the Sandinistas and Moscow and Cuba intended that. And they didn't die, they grew in strength and numbers and effectiveness as a consequence. And I think that is a good thing. . . .

I get the sense that somehow or another we've tried to create the impression that Oliver North picked up his hat and wandered around Washington and foreign capitals begging for money, and I didn't do that. I didn't have to do it because others were more willing to put up the money than the Congress because they saw well what was happening to us in Central America, and the devastating consequences of a contra wipeout and an American walkaway and write-off; to what was going to happen to this country and to democracy elsewhere in the world.

I didn't have to wander around and beg. There were other countries in the world, and other people in this country, who were more willing to help the Nicaraguan resistance survive, and cause democracy to prosper in Central America, than this body here. And that is an important factor in all of what you do, counsel, and in what this committee is going to do. It's got to be part of your assessment, as to why is it that other countries in the world were willing to step up and help in a desperate cause when we were not willing to do so ourselves.

That has got to be something that is debated not just by pulling people before this group and hammering at them and haranguing them and reducing it to pettiness. It has got to be something that the American people come to understand, how desperately important it was not just to us, not just to Ollie North and not just to President Ronald Reagan. It was important to these other people who put forth that money. And I didn't beg them, they offered. And that's important, sir. . . .

JULY 8, 1987

Q You testified about Admiral Poindexter and the President. Who else, if anyone—and I don't mean to imply anything in the question. But leaving those two people aside,

who else in the Government was aware of either the plan or the fact of using proceeds of arms sales to Iran for the contras?

A Well I, if I may clarify what I testified to yesterday, it is my assumption the President knew and then I subsequently testified that I was told he did not know. I know that Admiral Poindexter knew. I know that Mr. McFarlane knew at a point in time when he was no longer in the Government. And [CIA] Director [William J.] Casey knew.

Aside from that, I can't speak with certainty as to who else, inside the government, knew for sure. . . . But the only ones that I know for sure, who I confirmed it with, were those three. . . .

Q When did Director Casey first learn of it?

A Actually, I—my recollection is Director Casey learned about it before the fact. Since I'm confessing to things, I may have raised it with him before I raised it with Admiral Poindexter. Probably when I returned from the February—from the January discussions.

Q You're referring now to the discussions, the trip, during which you had the discussion with Mr. [Nanucher] Ghorbanifar [a go-between in the Iranian arms deal] in the bathroom?

A Yes, I don't recall raising the bathroom [discussion], specifically, with the Director, but I do recall talking with the Director and I don't remember whether it was before or after I talked to Admiral Poindexter about it. But I—I was not the only one who was enthusiastic about this idea. And I—Director Casey used several words to describe how he felt about it, all of which were effusive.

He referred to it as the ultimate irony, the ultimate covert operation kind of thing, and was very enthusiastic about it. He also recognized that there were potential liabilities. And that there was risk involved. . . .

Q What kinds of risks did he identify to you?

A This very political risk that we see being portrayed out here now; that it could indeed be dangerous, or not dangerous so much as politically damaging.

Q Do you have any reason to believe that Director Casey, given the political risk, ever discussed the matter with the President?

A I have no reason to believe that he did because he never addressed that to me. I never, as I indicated yesterday, no one ever told me that they had discussed it with the President. . . .

Q And there came a time, did there not, when you had an interview with members of the House Intelligence Committee?

A I did. . . .

Q And they were interested in finding out the answers to the questions raised by the resolution of inquiry?

A Exactly.

Q Your fund-raising activities, military support for the contras?

A That's right. . . .

Q But I take it you did considerably more which you did not tell the committee about?

A I have admitted that here before you today. . . . I will tell you right now, counsel, and all the members here gathered, that I misled the Congress. . . .

Q You made false statements to them about your activities in support of the contras?

A I did. Furthermore, I did so with a purpose. And I did so with the purpose of hopefully avoiding the very kind of thing that we have before us now, and avoiding a shut-off of help for the Nicaraguan resistance, and avoiding an elimination of the resistance facilities in three Central American countries, wherein we had promised those heads of state on my specific orders—on specific orders to me I had gone down there and assured them of our absolute and total discretion.

And I am admitting to you that I participated in the preparation of documents to the Congress that were erroneous, misleading, evasive and wrong. And I did it again here when I appeared before that committee convened in the White House Situation Room. And I make no excuses for what I did. I will tell you now that I am under oath and I was not then.

Q We do live in a democracy, don't we?

A We do sir, thank God.

Q In which it is the people not one marine lieutenant colonel that get to decide the important policy decisions for the nation?

A Yes, and I would point out that part of that answer is that this marine lieutenant colonel was not making all of those decisions on his own. As I indicated yesterday in my testimony, Mr. Nields, I sought approval for everything that I did.

Q But you denied Congress the facts?

A I did.

Q You denied the elected representatives of our people the facts, upon which, which they needed—

A I did.

Q —to make a very important decision for this nation?

A I did, because of what I have just described to you as our concerns. And I did it because we have had incredible leaks from discussions with closed committees of the Congress.

THE CONGRESSIONAL COMMITTEE HEARD FROM REAR ADM. JOHN M. POINDEXTER. HERE ARE EXCERPTS FROM HIS TESTIMONY, AS RECORDED BY THE NEW YORK TIMES

JULY 15, 1987

Arthur L. Liman, chief counsel to the Senate committee.

Now let's turn to the Iran initiative. Were you advised sometime in August of 1985 by Mr. McFarlane that the President had approved some Israeli transactions with Iran?

Admiral Poindexter Mr. Liman, that is a very fuzzy time period for me. . . . The period of time you're asking about, August of 1985, I was the deputy, and I did not have primary responsibility on this issue. . . .

Q But you did become aware that there was an Iran initiative?

A Yes, I did.

Q And you became aware of that from a conversation with Mr. McFarlane?

A I did. . . .

Q Now, admiral, did there come a time in connection with this transaction, when the C.I.A. sent over to you a proposed finding for the President to sign?

A Yes, Mr. Liman. That is the finding that I discussed with you earlier on the second of May.

Q Did you receive the letter of Nov. 26, 1985, from William Casey addressed to you which says, pursuant to our conversation, this should go to the President for his signature and should not be passed around in any hands below our level?

A I did receive that.

Q And you received the finding with it. Is that correct?

A Well, I must say that I don't actually remember getting it, but I'm sure that I did. I'm sure they came together.

Q Now, Admiral, when you saw the finding, am I correct that the finding itself was essentially a straight arms-for-hostage finding?

A That is correct. It had been prepared essentially by the C.I.A. as a what we call a C.Y.A. effort.

Q Did the President of the United States sign that finding?

A As I've testified before, he did, on or about the 5th of December. I'm vague on the date. . . .

Q Do you recall who was present when the President signed the finding?

A No, I don't. One of the reasons that I think my recollection is very poor on the circumstances of the President's actually signing this is that, recall that, that was a day or so after Mr. McFarlane had resigned and the President had just—I guess we had announced it on the fourth. Mr. McFarlane actually resigned, I think, on the 30th of November, we announced it on the fourth of December, and my recollection is that he signed this the following day on the fifth. My recollection now is that the C.I.A., especially the Deputy Director, John McMahon, was very anxious to get this signed. I frankly was never happy with it, because it was not fully staffed, and I frankly can't recall when I showed it to the President who was there or exactly what the discussion was or even what I recommended to him at this point. I simply can't remember that.

Q But you do recall that whatever you recommended, the President read it and he signed it.

A Yes, he did. He did sign it.

Q And there was, in fact, the recommendation from Bill Casey that he sign it, and Bill Casey was a person whose advice the President valued.

A He did.

Q Now what happened to that finding?

A As I said earlier, I destroyed that by tearing it up on the 21st of November because I thought it was a significant political embarrassment to the President. And I wanted to protect him from possible disclosure of this. To get into the details of exactly how it happened, which I assume you're interested in—

Q Yes. When you say the 21st of November, you're talking about the 21st of November 1986.

A 1986. That's correct.

Q Now, would you tell the panel the circumstances of your destroying this finding because you thought it would be a significant political embarrassment to the President?

A I will. The finding, the existence of the finding I had completely forgotten in early November 1986. As I said before, the finding initially was prepared by the C.I.A. for the reason that I stated. I can recall in my time at the White House one or possibly two other findings that had a retroactive nature to them. I frankly was always uncomfortable with that because I thought it didn't particularly make a lot of sense.

The finding was very narrow. It was prepared before there had been thorough discussion of the issue. As I said earlier, I came into the issue in a full, responsible way in early December of 1985. Prior to that time, Mr. McFarlane had handled it. I felt that it was important that we improve on this finding so that we clearly lay out what the objectives were in the Iranian . . . After this finding was signed, it was retained in my immediate office and at some point after it was signed I had apparently given it to Commander Thompson, my military assistant, to put in an envelope in his safe to keep.

I had, as I said, completely forgotten about it. On November the 21st, when Ed Meese [the Attorney General] called me and said—well, to go back a step, we'd run into a problem in November of what had actually happened in 1985. It was very dim in people's memories. We didn't think we had much in writing.

As I think you've heard Colonel North testify, we frankly did not realize the old PROF notes [the White House electronic message system] existed. My policy was to erase them, and I apparently did it the right way, and I don't think Colonel North did it the right way. So we didn't have the benefit that these committees have in going back over these old PROF notes, or we didn't realize that we had that opportunity.

But Ed Meese and I talked many times during the month of November, and when it became clear that there was a disagreement between Cabinet-level officials as to what had happened in November of 1985, he indicated that he wanted to come over and ask the President to have a fact-finding session primarily with the Cabinet-level officials involved to try to sort out what had happened, actually happened in November of 1985. And he called me early in the morning on the 21st of November and told me this, and he said he had an appointment to see the President at 11:30, and he wanted me and Don Regan [the White House chief of staff] to go with him, which we did at 11:30.

He told the President about the controversy, not really controversy, the different recollections as to what had happened in November. And he said he thought it would be useful if he would have a couple of his people that were close to him look into the matter to see if they could piece together what had happened. The President readily agreed. . . .

So Ed called me after lunch. . . . and he asked if I would have the appropriate documents pulled together so they could take a look at them. I said I would do that. After he called, I called Commander Thompson, my military assistant, and asked him to take charge of pulling these documents together.

And then I called Colonel North and told him of my conversation with Mr. Meese and asked him to cooperate with Commander Thompson and Mr. Meese's people. . . .

Later in the afternoon or early evening, Commander Thompson brought into my office the envelopes that I had given him earlier containing the material we had on the

Iranian project in the immediate office, which was essentially the various findings. And he pulled out this November finding—it was actually signed in December. And my recollection is that he said something to the effect that they'll have a field day with this, or something to that effect. . . . The import of his comment was that up until that time in November of 1986, the President was being beaten about the head and shoulders, that this was, the whole Iranian project, was just an arms-for-hostage deal.

Well, this finding, unfortunately, gave that same impression. And I, frankly, didn't see any need for it at the time. I thought it was politically embarrassing, and so I decided to tear it up. And I tore it up, put it in the burn basket behind my desk.

I can't recall, but I believe that Colonel North was there in the office, but I'm a little fuzzy on that point.

Q Was Commander Thompson there when you tore it up?

A I believe he was, but I can't swear to it. I know he brought it in, and I can recall his comment, but exactly how long it took me, because I—when he made his comment he said, I said, well let me see the finding. And he pulled it out and gave it to me, and I read it and at some point after that I tore it up, but it was within a short period of time.

Q Admiral, you talked about the fact that the President was being beaten around the head and shoulders by the media for sanctioning an arms-for-hostage deal and that this finding seemed to corroborate it, and you therefore destroyed it in order to prevent significant political embarrassment. Did you regard one of the responsibilities of the national security adviser to protect the President from political embarrassment?

A I think that it's always the responsibility of a staff to protect their leader and certainly in this case where the leader is the Commander in Chief. I feel very strongly that that's one of the roles. And I don't mean that in any sense of covering up, but one has to always put things in the President's perspective and to make sure that he's not put in a position that can be politically embarrassing.

Q Now, Admiral, a finding represents a decision of the President of the United States, correct?

A A finding, I don't believe, is discussed in any statute. It is discussed in various Presidential directives. It is an artifact of what the statute calls a Presidential determination.

Q And the President, when he signed this finding, was making a determination?

A That's correct, but it's important to point out that the finding, that early finding was designed for a very specific purpose, and was not fully staffed and did not in any way ever represent the total thinking on the subject.

Q The President didn't authorize you to destroy the finding, correct?

A He certainly did not.

MEETING OF THE N.S.C.

Q Let's go to the—on Dec. 7, 1985, after the finding had been signed by the President, there was a meeting, was there not, between the principals of the National Security Council?

A Yes, there was.

Q And you recall Mr. Weinberger was there, and Secretary Shultz was there, Don Regan was there, Mr. McMahon of the C.I.A. was there, do you recall that?

A Yes, I do.

Q . . . At this meeting, there was a discussion again, or there was a discussion of the Iran initiative? Is that so? . . .

A Yes, yes, there was. . . .

Q And the subject on the table was an Israeli initiative, under which the Israelis would ship arms to the Iranians and we would replenish the arms. Hopefully there would be better relations with Iran. And as a token of good faith, the American hostages would be released. Is that a fair summary?

A Well, I think it's a partial summary.

Q Well, why don't you complete it?

A We had been concerned, in the National Security Council, for some period of time, with the situation in Iran. Unfortunately, we have very poor intelligence on what's happening in Iran. The National Security Council staff had prepared a draft finding, earlier in 1985, to try to get the Government focused on what we saw as a very significant, looming problem in Iran, as Ayatollah Khomeini eventually passed from the scene and there was some sort of succession.

We didn't want a repeat of the 1970's, when things were happening in Iran that we weren't aware of, and eventually went out of our control, and out of control of the Government there.

. . . We felt that we needed to take an initiative to get closer to people in the Iranian Government, so that we could find out what's happening and hopefully have some influence in the future or, at least, have information on which to base the United States policy.

Q Admiral, see if this part is correct: that the currency for trying to get that influence that was being demanded, as reported by the Israelis, involved arms?

A That is often the currency of any sort of business in the Middle East.

Q And in this case that was the currency being demanded?

A Yes, that is correct.

Q And it is also true that we did not want to authorize arms shipments to the Iranians, unless we were assured of getting our hostages back, is that so?

A As I was trying to lay out a moment ago, what our concerns were, what our major objective was, the President was clearly also concerned about the hostages. The President is a very sensitive person, and he is concerned about individuals when they're in difficulty. And so he, just as a human being, was concerned about the hostages.

I don't think that the President is overly concerned about them, but he recognized that we did have an opportunity here to try to get the hostages back. And there was no way that we could carry on discussions with Iranian officials about broader objectives, until we got over the first obstacle. And the first obstacle was to get the hostages back. And the President felt that, that it was worth taking some risks here.

Q Now, did the Secretary of State and the Secretary of Defense express objections?

A They expressed, as opposed to some reports, very strong, vociferous objection and clearly laid out for the President the other side of the issue.

Q And without going into undue detail, could you just tick off the points they made?

A Well, there are the obvious points that have been made since this all has become public. Secretary Shultz was concerned about our operation to staunch the flow of arms into Iran, which is one of the methods that we are using to try to stop the war between Iran and Iraq. . . .

But in its simplest terms, what was being proposed here was not in accordance with that particular method that we were using. He was concerned that if the European countries found out about it, that it would lessen their willingness to cooperate. In reality though, in my opinion, we've never had good cooperation from anybody on Operation Staunch. The European countries continue to send military equipment and supplies into Iran. Iran's been able to carry on the war for six, going on seven, years now, I guess.

Other objections were that of it was contrary to the Arms Export Control Act. Secretary Weinberger had slightly different reasons, but they're generally along the same lines.

Q And there's no doubt in your mind that the President listened to, and understood, those objections?

A . . . The President listened to all of this very carefully. And at the end of the discussion, at least the first round, he sat back and he said something to the effect—and I, this is not a direct quote—but it was something to the effect that, I don't feel that we can leave any stone unturned in trying to get the hostages back. We clearly have a situation here where there are larger strategic interests. But it's also an opportunity to get the hostages back. And I think that we ought to at least take the next step. . . .

Q Now, one other question which just has been handed to me, that Colonel North apparently testified that Secretary Shultz and Secretary Weinberger's opposition was not vigorously expressed in this January period. I take it that it was vigorously expressed at the January 7th meeting, and it was expressed by the Secretary of State at that January 16th meeting and that no one had any doubt about where both of them stood.

A That's true of the earlier meetings. On the 16th of January, I think it was pretty clear to George [Shultz] that the President wanted to go ahead with this at that point, and so although he voiced objection, I wouldn't say that, and this is probably why Colonel North's recollection is as it was. In fact, I think probably the 16 January meeting may have been the only meeting that Colonel North was in attendance where he may have heard the other Cabinet officers give their views. But it is accurate that both George Shultz and Cap Weinberger vigorously made this case as to why we should not do this.

LEGALITY AND APPROVAL

Q Right. Now, admiral, is it correct that in the discussions that you had leading up to the January 17th finding, there was no discussion with the President of the United States about the possibility of using proceeds of the sale to support the contras?

A There was none.

Q And there was none with you.

A There was none with me.

Q Now, would you tell us, and I'm going to break this into different questions, when was the first time that you were told by Colonel North about this possibility?

A My best recollection is that this took place sometime in February of 1986.

Q And would you tell us what Colonel North said to you?

A My recollection is that he had just come back from a meeting in London, and he was giving me a general update on the situation as he saw it. And he was reviewing the status of the work that was in progress at C.I.A. and Defense in addition to the results of his meeting in London. And near the end of the conversation, my recollection is that he said something to the effect that, Admiral, I think we can, I have found a way that we can legally provide some funds to the democratic resistance or as they have been called here—and I frankly agree with Congressman [Henry J.] Hyde [R.-Illinois] that I have no problem with calling them contras—through funds that will accrue from the arms sales to the Iranians.

Q Did he use the word legally?

A My best recollection is that he did, but of course I know that Colonel North is not a lawyer, and so I was taking that in a layman's sense that that was his conclusion.

Q Do you recall in reciting this in your deposition you didn't use the word legally?

A I don't recall that, that I didn't. I believe that he did, he may not have.

Q Now, did he tell you what the method would be for doing this?

A This was a very general discussion, but this was clearly a new aspect that I had not thought about before. To make a long story short, in the end I thought it was a very good idea at the end of this conversation, and I personally approved it.

Q Did he ask you for your approval?

A I don't recall how he phrased his request, but he was clearly looking for a signal from me whether or not to proceed ahead along this line.

Q And you gave it.

A And I gave it to him. . . .

In order to put this in perspective, and I think it's important to understand my state of mind at the time and what things were of concern to us. The President's policy with regard to support for the contras had not changed since 1981. The various versions of the Boland Amendment came and went. But the President was steadfast in his support for the contras. . . . So 1was absolutely convinced as to what the President's policy was with regard to support for the contras.

I was aware that the President was aware of third-country support, that the President was aware of private support. And the way Colonel North described this to me at the time, it was obvious to me that this fell in exactly the same category that these funds could either be characterized as private funds because of the way that we had, that Director Casey and I had agreed to carry out the finding. They could be characterized as private funds or they could be characterized as third-country funds. In my view, it was a matter of implementation of the President's policy, with regard to support for the contras.

We were in the process of working on our legislative plan to get $100 million from Congress for essentially unrestricted support to the contras. . . .

The President was bound and determined and still is, that he will not sit still for the consolidation of a Communist government on the mainland of America. And in

order to prevent that, he feels that the most effective way, with which I also agree, is to keep pressure on the Communist Sandinista Government. And the most effective way to do that, given all of the factors considered and because we don't want to send U.S. soldiers to Nicaragua, is to provide support to the contras and keep them alive until we can get the $100 million. . . .

And so after weighing all of these matters—and I also felt that I had the authority to approve it because I had a commission from the President which was in very broad terms. My role was to make sure that his policies were implemented. In this case, the policy was very clear, and that was to support the contras. After working with the President for five and a half years, the last three of which were very close and probably closer than any other officer in the White House except the chief of staff, I was convinced that I understood the President's thinking on this and that if I had taken it to him that he would have approved it.

Now I was not so naïve as to believe that it was not a politically volatile issue; it clearly was because of the divisions that existed within the Congress on the issue of support for the contras. And it was clear that there would be a lot of people that would disagree, that would make accusations that indeed have been made. So although I was convinced that we could properly do it and that the President would approve if asked, I made a very deliberate decision not to ask the President so that I could insulate him from the decision and provide some future deniability for the President if it ever leaked out. Of course, our hope was that it would not leak out.

Q When you say deniability, are you saying that your decision was not to tell the President so that he would be able to deny that he knew of it?

A That's correct.

Q And did you at any time prior to the Attorney General's finding this on November 22d tell the President of the United States of the fact that proceeds from the Iranian arms sale were being used to support the contras?

A I don't—I did not. I want to make this very clear because I understand it's an important issue. I did not talk to anybody else except Colonel North about this decision until, to my knowledge, my best recollection—and I don't want to quibble here over times in late November 1986—but my recollection is the first mention that I made to anybody besides Colonel North was on November 24, 1986, to Ed Meese.

Q And so that the answer is you did not tell the President of the United States.

A I did not.

Q And that for a period of whatever it is, nine months, you kept it from the President of the United States, for the reasons you've given.

A Mr. Liman, this clearly was an important decision but it was also an implementation of very clear policy. If the President had asked me, I very likely would have told him about it. But he didn't. And I think—you know, an important point here is that on this whole issue, you know, the buck stops here with me. I made the decision; I felt that I had the authority to do it. I thought it was a good idea. I was convinced that the President would in the end think it was a good idea. But I did not want him to be associated with the decision. . . .

Q Were there any other examples during your term as national security adviser where you withheld a decision from the President that you had made in order to give him deniability?

A Well, this again—this decision, in my view, was a matter of implementation, and there were many details of implementation that were not discussed with the President. This particular detail was the only one of its kind in terms of the disagreements and the controversy that existed over the issue.

Q Were there any other decisions that you withheld from the President that you had made because they were politically explosive?

A I don't recall anything else that fell in that same category, although there were lots—I want to make a distinction here between what I felt my authority was and why I didn't discuss it with the President. Number one, I felt that it was within my authority because it was an implementation of a policy that was well understood, that the President felt very strongly about. It was not a secret foreign policy, the President's policy with regard to the contras was clearly understood by every member of the Congress and the American people. So it wasn't matter of going out and making a secret foreign policy. . . .

You know, frankly, as Colonel North has testified, I thought it was a neat idea, too. And I'm sure the President would have enjoyed knowing about it. But on the other hand, because it would be controversial—and I must say that I don't believe that I estimated how controversial it would be accurately—but I knew very well that it would be controversial, and I wanted the President to have some deniability so that he would be protected and at the same time we'd be able to carry out his policy and provide the opposition to the Sandinista Government. . . .

AIDING THE CONTRAS

Q Now as I understand your testimony, you genuinely believed that in approving the diversion, that it was consistent with the policies of the President, in terms of third-country support. You've already testified to that. And I'd like to ask you some questions about that. Is it a fact that the Administration had gone to Congress in 1985 and gotten permission from Congress to solicit third-country support?

A Yes, we worked with members of Congress to get that provision.

Q And is it a fact that that provision for obtaining third-country support was limited to humanitarian aid?

A Since leaving the White House and going back over this material, that is correct. I can't say that during the discussions, that I can recall in the White House, there was great distinction made between humanitarian aid or any other kind of aid, at that particular time. There was with respect to the $27 million. But I just simply don't recall great distinctions being made.

Q Well, are you saying that when Congress worked out the legislation with the Administration that authorized solicitation for humanitarian aid, the Administration interpreted that as meaning that it could solicit for lethal aid?

A No, I'm not saying that at all. I'm just giving you my recollection of the time.

Q Now, and you also understood that that bill provided that it was only the State Department that could do the solicitation, do you recall that, sir?

A Yes, I recall that.

Q Now, was the money that you were getting from the Ayatollah, or [Gen. Richard]

Secord [another go-between], however you viewed it, was that money to be limited to being disbursed for humanitarian aid?

A In no way. You see the distinction here is that—and this is contrary to what you have heard before, from other witnesses. But I never believed, and I don't believe today, that the Boland Amendment ever applied to the National Security Council staff or the President's personal staff. But the problem was that the Boland Amendment did apply to the State Department. It did apply to C.I.A. And it did apply to the Defense Department.

We had been running this operation, on our own, for a long period of time because there was no other alternative, in order to keep the contras alive. And we wanted help. We wanted also a more public recognition of the fact that the U.S. was supporting the contras in some way.

I frankly, I personally still wanted that to be done in—the public support to be done in such way that we could slowly turn back to a covert program, run by the C.I.A. But it was important to me, and to others, that we get the State Department back into the game.

Q I understand you. Did you ever discuss, with the President of the United States, that the N.S.C. was raising money for lethal aid?

A Mr. Liman does—are you, if I may ask to clarify the question—are you saying that raising money is soliciting money?

Q I don't want to get into a semantic debate about solicitation. I mean every day in the newspapers, in the financial sections, they have announcements of offerings, and they say this is not a solicitation. So please do not get me into that semantic debate. Let's talk about raising money, obtaining money, for lethal aid. That the N.S.C. was obtaining money for lethal aid?

A The President was aware that we were encouraging, I guess would be a fair way to describe it, third countries to contribute to the cause of the contras in Central America, in their fight against the Communist Sandinistas. And, of course, we were doing that primarily by pointing out to them the dangers that we saw. And, as Colonel North has testified, it wasn't very difficult. They clearly understood the problem. The Central American countries understood, the neighboring countries. The other countries that are on your list, that I've heard you talk about up here. . . .

FINANCING COVERT PROJECTS

Q Colonel North testified that in addition to the use of the proceeds of the Iranian arms sale for the contras, it was to be used for a series of other covert projects. Do you remember that testimony of his?

A I heard that testimony.

Q Was that the first time you ever heard about that?

A It's the first time that I heard it discussed in that depth. I must say there was, as far as I was concerned, no such plan. I don't at all doubt that Colonel North and Director Casey may have discussed that. Frankly, it's an idea that has some attractive features in my mind, but there was no plan that was brought to me or that I took to the President to proceed in that kind of direction. That would have required substantial discussion. . . .

Q You testified this morning that if the President had asked you about what countries were helping, you probably would have told him about this. Do you recall that?

A That would have been a difficult situation, and I don't—

Q But you wouldn't lie to the President?

A I wouldn't lie to the President, and if he had outright asked me about it, I would have told him. He didn't.

Q Are you saying that with the interest the President had in the contra movement and his concern about the dire straits it was in financially that he never asked you which countries were helping?

A That's correct. The President is—as I've said—is not a man for great detail. He—and I don't mean that in any sort of funny way—I don't think a President ought to get involved in details—he has to maintain a strategic perspective, and he's got enough to worry about. I think by and large the President has the same sort of management philosophy that I do, and that is that he picks good people for the job and gives them a lot of authority to carry out that job, and he wanted the contras supported. We were reporting to him on the status of the contras, in general terms, and he knew that they were surviving and that was the thing that was important to him.

AT THE CONCLUSION OF POINDEXTER'S APPEARANCE, REPRESENTATIVE LEE H. HAMILTON, DEMOCRAT OF INDIANA, THE CHAIRMAN OF THE HOUSE COMMITTEE, ADDRESSED HIM ABOUT HIS TESTIMONY DURING THE HEARINGS:

JULY 21, 1987

Representative Hamilton. . . . Admiral Poindexter, I want to say that we have indeed appreciated your testimony. . . . None of us, I think, can know all of the circumstances that you confronted as the national security adviser to the President.

. . . It is, however, . . . our job to examine your role in the decision-making process. . . .

Now, your comments about secrecy in government . . . concerned me . . . a great deal. You have testified that you intentionally withheld information from the President, denied him the opportunity to make, probably, the most fateful decision of his Presidency—whether to divert the funds from the Iranian arms sales to aid the contras.

You said your objective was to withhold information from the Congress. And apparently, so far as I understood the testimony, without direction or authority to do so. As many have mentioned, you destroyed the Dec. 5, '85, finding. You apparently intended to have original documents, relating to the contras, either altered or removed. You were unwilling to speak candidly with senior Justice and C.I.A. officials about the Hawk missile shipments to Iran. And you kept the . . . Secretaries of State and Defense, uninformed. . . .

All of us who work with our system of government sometimes feel impatient with its painstaking procedures. . . . Yet, your comment about Congress, and I quote it directly: I simply did not want any outside interference, reflects an attitude which makes, in my judgment at least, our constitutional system of checks and balances unworkable.

Instead of bringing each agency dealing with foreign policy into the process, you cut those agencies out of the process. You told the committees, I firmly believe in very tight

compartmentation. You compartmentalized not only the President's senior advisers, but in effect, you locked the President himself out of the process.

You began your testimony by saying that the function of a national security adviser is to present options and to advise the President. Yet, you told the committees the buck stops here with me. That is not where the buck is supposed to stop.

You wanted to deflect blame from the President but that is another way of saying you wanted to deflect responsibility from the President. And that should not be done in our system of government.

You testified that diverting funds to the contras was a detail, a matter of implementation of the President's policies. And you felt that you had the authority to approve it. Yet, this was a major foreign policy initiative, as subsequent events have shown, with very far-reaching ramifications. And this member, at least, wonders what else could be done in the President's name, if this is mere implementation of policy. . . .

Probably more important, secrecy contributed to disarray in the Oval Office. The President apparently did not know that you were making some of the most important foreign policy decisions of his Presidency. You've testified, I was convinced that the President would, in the end, think the diversion was a good idea. Yet, the President has stated that he would not've approved the diversion.

Excessive secrecy placed the President in an untenable position and caused him to make false and contradictory public statements. Let me cite some of them:

On Nov. 6, 1986, the President said, the speculation, the commenting and all, on a story that came out of the Middle East has no foundation.

A week later, the President said, we did not, repeat, we did not, trade weapons, or anything else, for hostages.

But on March 4, the President said: A few months ago, I told the American people I did not trade arms for hostages. My heart and my best intentions still tell me that's true but the facts and the evidence tell me it is not.

Turning to the solicitation of private aid for the contras, the President said, on May 5, I don't know how that money was to be used. And I have no knowledge that there was ever any solicitation by our people with these people.

But on May 15, the President altered his view. He said: As a matter of fact, I was definitely involved in the decisions about support to the freedom fighters. It was my idea to begin with.

May I suggest that the President was unaware of some important actions taken by his staff and, therefore, he misspoke. Because he lacked information, the President inflicted serious and repeated political wounds upon himself. Polls continue to indicate that a majority of the American people still feels that the President, despite his statements to the contrary, did know that money from the Iran arms sales was channeled to the contras. . . .

POINDEXTER I just have one brief comment.

HAMILTON Yes, indeed.

POINDEXTER Mr. Chairman, with regard to your closing statement I would just simply say that we'll have to agree, you and I, to disagree on your interpretation of many of the events. And finally, I leave this hearing with my head held high that I have done my very best to promote the long-term national security interests of the United States. Thank you.

FOLLOWING ARE EXCERPTS FROM SECRETARY OF STATE GEORGE P SHULTZ'S TESTIMONY:

JULY 24, 1987

Representative Lee H. Hamilton, chairman of the House committee. Mr. Secretary, do you have an opening statement?

MR. SHULTZ No, I don't. But with your permission, Mr. Chairman, I'd like to make a few remarks.

Q Please proceed.

A . . . I have on numerous occasions—including, I think, before your committee right here, Chairman [Dante B.] Fascell [D.-Florida, chairman of the House Foreign Affairs Committee]—been asked about what advice I gave the President on this, that or the other, subject. And I have always taken a position, in 10 and a half years as a member of the Cabinet, that those conversations are privileged and I would not discuss them. This is an exception, and I have made this material available on the President's instruction. But I mention it because if I'm testifying before you on some other subject sometime and you try to use this as a precedent, I won't buy it. I'm just putting you on notice right now.

Thank you, Mr. Chairman.

Q Thank you, Mr. Secretary. We'll begin the questions this morning with Mr. Belnick. . . .

Mark A. Belnick, executive assistant to the chief counsel of the Senate committee. Mr. Secretary, I'd like to begin this morning by reviewing certain key events that the panel has been considering in order to establish when the Secretary of State was first informed of those events. . . .

Let me begin by this question. Mr. Secretary, when were you first informed that the President of the United States had signed a covert action finding authorizing the sale of U.S. arms to Iran?

A On November the 10th, 1986, at a meeting in the Oval Office, with the President's principal advisers, during a briefing by Admiral Poindexter on what had transpired over the past year or so. . . .

Q Mr. Secretary, when were you first informed that this nation had sold weapons directly to Iran?

A . . . This all started to break in very early November 1986. . . .

Q Prior to then, . . . had any member of the United States Government informed you that the United States had sold weapons directly . . . to Iran?

A No.

Q Mr. Secretary, when were you first informed of the McFarlane mission to Teheran?

A It was after the mission, but I think shortly after it was completed.

Q And were you given the details of the mission at that time?

A I was told that it had fizzled, . . . that the whole project had been told to stand down.

Q Were you told at that time that Mr. McFarlane had brought U.S. weapons with him to Teheran?

A No. . . .

Q Mr. Secretary, when were you first informed that United States negotiations with the second channel in the early autumn of 1986 had produced agreement on a so-called nine-point agenda which provided for additional arms sales to Iran in exchange for hostages and which contained provision also with respect to actions directed at the Government of Iraq?

A On December 13th of 1986. But if I may interrupt your questioning, I'd like to expand on that.

Q Please.

A In the course of the effort to come to grips with what was taking place, the President put the management of Iran matters into my hands by that time—we're talking in December—sort of at first a little bit but then for sure. And I discovered that the C.I.A. had a meeting scheduled with an Iranian for that date. And so we considered what to do. And we decided that we should go ahead with that meeting, that the C.I.A. representative who was scheduled to be the representative there, Mr. Cave, should go. But we would have accompanying him Mr. Charles Dunbar, who is a Foreign Service officer and Farsi speaker. And we would have instructions carefully written, designed to use the meeting as a means to tell that channel that there would be no more arms sales discussed in that channel or anywhere else. . . .

At the meeting, the message was delivered, but also as our representative listened, there was back and forth discussion about this agenda, nine-point agenda. And so gradually then, and in discussion with Mr. Cave, Mr. Dunbar got a reasonable idea of what was on this agenda. And then he called that back on Dec. 13, which was a Saturday, to the department. And I saw it on Saturday afternoon. And it was astonishing.

So I called the President, or I called the White House to get an appointment with the President. And there was a lot of back and forth, what did I want to see him about and so on. And I didn't seem to be getting an appointment right away, so I picked up the phone Sunday morning and I called the President. I said, "Mr. President, I have something I should bring over here and tell you about right now." So he said, 'Fine, come over.' He happened to be in Washington.

I went up to the family quarters, and Al Keel, who was then acting national security adviser, went with me, at my request. And I told the President the items on this agenda, including such things as doing something about the Dawa prisoners, which made me sick to my stomach that anybody would talk about that as something we would consider doing.

And the President was astonished. And I have never seen him so mad. He's a very genial, pleasant man and doesn't—very easy-going. But his jaw set, and his eyes flashed, and both of us, I think, felt the same way about it. And I think in that meeting I finally felt that the President deeply understands that something is radically wrong here. . . .

Q . . . In particular, Admiral Poindexter testified that he did not withhold anything from you that you did not want withheld from you. . . . Mr. Secretary, . . . let me ask you first whether you ever told Admiral Poindexter or any other member of the Administration that you did not want to be kept informed of the Iran initiative?

A I never made such a statement. What I did say to Admiral Poindexter was that I wanted to be informed of the things I needed to know to do my job as Secretary of State, but he didn't need to keep me posted on the details, the operational details of

what he was doing. That's what I told him. . . . The reason for that was that there had been a great amount of discussion of leaks in the Administration, and justifiably so. And we were all very concerned about it. And there had been in connection with what to do about it, discussion of the idea of giving very large numbers of people who were—who had access to classified information, lie detector tests on a regular or random basis, which I opposed.

While I was on a trip abroad in the latter part of 1985, a directive encompassing that idea was signed. So I didn't comment on it while I was abroad, but when I got back here I did comment on it, registered my opposition, talked to the President about it. And it got changed. Now that, I recognized, put me at odds with the intelligence and national security community, to put it mildly. So . . . in terms of particulars, like who is going to go someplace to meet somebody and so forth, . . . it seemed to me in the light of the suspicions cast on me as a result, and the hostility, that I would not know that. So I felt it would probably leak, and then it wouldn't be my leak. . . .

But that doesn't mean that I just bowed out insofar as major things having to do with our foreign policy are concerned. . . . To consider that that statement would mean that I shouldn't be informed of things like that is ridiculous. . . .

Q Do you recall what you told Admiral Poindexter about your views concerning the Iran initiative, as he described it to you in that briefing?

A Well, I told him that I thought it was a very bad idea, that I was opposed to it. . . . I was in favor of doing things that had any potential for rear-ranging the behavior of Iran and our relationship with Iran. But I was very much opposed to arms sales in connection with that.

Q Did you tell him at that time that in your view, the proposed policy amounted to paying for hostages and had to be stopped?

A Yes.

Q In that same conversation, sir, on Dec. 5, . . . did he tell you that on the very same day, the President had signed a covert action finding authorizing an arms shipment to Iran?

A No. . . .

Q Now do you recall another briefing, listed on the chronology by Admiral Poindexter a month later, on Feb. 28, in which he discussed the hostage situation and advised you then of a possible high-level meeting between Bud McFarlane and certain Iranian representatives?

A Yes, I do. He told me that as a result of the discussions they had been having, that the Iranians had said they wanted a high-level meeting and if there were a proper high-level meeting, discussing our future possible relationships, that would be the occasion in which hostages . . . would be released. I said, 'Well, that sounds almost too good to be true. But anyway, if that's the case, I'm in favor of it.' . . .

Q Did Admiral Poindexter tell you that the agenda for any meeting between Mr. McFarlane and Iranian representatives would include current deliveries of U.S. arms?

A No. . . . This negotiation had been taking place in a manner consistent with what I thought was proper, and I thought, well, maybe I won the argument after all, with the President.

Q In that light, did Admiral Poindexter tell you on Feb. 28 that only one day before, that was on Feb. 27, the United States had shipped 500 TOW's, TOW missiles, to Iran,

and that about 10 days earlier the United States had also shipped 500 TOW missiles to Iran?

A No, he did not. . . .

Q In May 1986, . . . you were advised . . . of an approach to a British entrepreneur by Mr. Nir about . . . an arms deal to Iran . . . which supposedly had White House approval which had John Poindexter as the point man and which included participants such as Mr. Adnan Khashoggi and Mr. Ghorbanifar?

A Yes. . . . I received a cable from the Under Secretary of State, Mr. Armacost, . . . in Tokyo. . . .

Q Once you received this information, you spoke to Don Regan . . . and Admiral Poindexter. Am I correct?

A That's correct.

Q I understand that in those conversations you objected strongly to any such deal, to the United States being involved, insisted that if there was such an operation it be called off and warned that the President was seriously exposed and at risk. . . . Is that a fair summary?

A Yes. . . . You can imagine how I felt when I read this cable. . . . I said more or less what you said. Don Regan seemed to me to be very upset about it. He said he would take it up with the President when he saw him. . . . He later told me that the President was upset and this was not anything he knew about. And Admiral Poindexter told me . . . we are not dealing with these people, this is not our deal. . . .

Q Well, when Admiral Poindexter told you that this was not our deal, . . . did he inform you that our deal involved an upcoming mission . . . to Teheran, which would be led by Bud McFarlane, which would include a shipment of Hawk spare parts to Iran?

A No. . . .

Q Also, Mr. Secretary, if I could, let me ask you to turn to exhibit 24. That exhibit, sir, is a PROF note dated May 17, 1986. . . . from Oliver North to Admiral Poindexter about the McFarlane mission to Teheran. . . . Colonel North suggests to Admiral Poindexter that there be a quiet meeting with Bud McFarlane and the President prior to the departure of the mission, and he queries whether the participants . . . ought to include you and the Secretary of Defense and the D.C.I. [Director, Central Intelligence: William J. Casey]. Do you see that?

A Yes, I see that.

Q If you turn, then, please, to the next exhibit, . . . you'll see Admiral Poindexter's reply to that suggestion, . . . and I quote, 'I don't want a meeting with R.R., Shultz and Weinberger.' . . . I take it you were unaware of this exchange, as well?

A Obviously. . . .

Q Mr. Secretary, you testified earlier, . . . that you had told Admiral Poindexter that while you didn't need to be informed of what you called operational details, you did want and need to be kept informed of those facts which you needed in order to do your job—correct?

A Correct.

Q Sir, in order to do your job as the nation's chief diplomat, and as a statutory member of the National Security Council, and at a time when, through Operation Staunch, you

were in charge of attempting to persuade our allies and other nations throughout the world not to sell arms to Iran, did you need to know that the United States itself was selling arms to Iran, that the President had signed covert action findings authorizing those sales, and that the President's former national security adviser was in Teheran on a diplomatic mission, bringing with him the first installment on the delivery of U.S. Hawk parts? Did you need to know those facts?

A Certainly. One of the many arguments that I used, and Secretary Weinberger used, in opposing having an arms sale dimension to the Iran initiative, one of the arguments, was that we felt that one way of getting the Iran-Iraq war to come to an end was to do everything we could to deny weapons to the country that was refusing to come to an end, and so we had a rather vigorous program, called Operation Staunch.

Q Sir, did you ever express the view that Colonel North was a loose cannon?

A No, I didn't. What I said—I think what you're referring to is an incident . . . in which I told Elliott Abrams [Assistant Secretary of State for Latin America]—the question was where, where are the freedom fighters getting their arms. . . . And Elliott said he didn't know. And I said, well, you're our pointman here, you should find out, or something like that.

Q As I understand, that conversation took place on Sept. 4, 1985. Secretary Abrams has described that conversation here, based on a note that he took, in which he said you told him to 'monitor Ollie.' Is that your recollection? . . .

A . . . No reason why Elliott shouldn't have taken it that way, because Colonel North was commonly seen as a principal contact with the freedom fighters.

Q Did you have a view at that time that Colonel North, because of any information that you had about him, was someone who had to be watched closely or that Elliott ought to monitor?

A There was talk around about erratic behavior on his part, but I had no particular knowledge about it and didn't want to pass judgment. . . . I can't get myself in the position of supervising people down the line working for others.

Q But you did expect, based on what you told Secretary Abrams Sept. 4, 1985, that he would keep himself informed about . . . how the contras were getting supplied with arms, and not simply shut his eyes to that?

A Yes.

Q All right, sir, in light of what you now know, . . . regarding, for example, the role of Colonel North and other N.S.C. staff members in assisting the contras during the period of the Boland restrictions, the involvement in the Hasenfus flight, the involvement of at least one of our own ambassadors, Mr. Tams, in negotiations for an airstrip to be used in Central America for contra resupply and in helping, as he testified to this panel, on instructions from Colonel North, to open a southern military front against Nicaragua, during the period of the Boland restrictions, . . . is it your view that Secretary Abrams carried out your instruction to keep himself, and you, informed?

A What has been brought out, in these hearings about all of the activities you mentioned, has surprised a lot of people. It surprised me. It must have been a surprise to Chairman Hamilton, who looked into this a couple of times and had assurances. So I imagine it has surprised the President. So things have come out that we didn't know about. . . .

Senator Daniel K. Inouye, chairman of the Senate Committee. Mr. Secretary, at the outset of these hearings, which began about two months ago, I made a sad prediction that when the story began to unfold, the American people will have the right to ask, how did this ever happen here? Or, how could this ever happen in the United States? And I think, at the same time, Americans would have the right to demand that it never happen again.

The story we have heard over the past 10 weeks of testimony, to some has been sad and depressing and distressing, and to many of us on this panel, many of us old-timers and a bit sophisticated, but we found it shocking and at times frightening.

And I believe that made the question that the Americans will ask, and the expectations they have, a bit more compelling.

Mr. Secretary, you and I have lived through the agony and the nightmare of Watergate. And we saw it ruin a President, ruin his senior advisers, demoralize the country and cause the American people to lose faith in their political leaders.

And therefore, it's especially troubling to me, and I'm sure it's to you, to see this nation once again faced with this breakdown of trust, between the important branches of Government, and more importantly, between the Government and the American people. . . .

My question is a very general one, Mr. Secretary, but with your background in public service and being at the helm of the State Department, I hope you can give us a response. How did this happen again? And how did life-long public servants, and patriotic Americans, like Admiral Poindexter, Bud McFarlane and Bill Casey and Oliver North, find themselves in a position where they misled you, kept information away from the Secretary of State, from the Secretary of Defense, lied to the Congress, withheld information from the President of the United States, destroyed . . . Government documents to hide or cover up their activities, and involved rather shady characters—and that's an understatement, I think—in participating in the formulation of foreign policy, and the implementation of such, while, at the same time, skirting around the people who should be doing that work, to wit, the Secretary of State and the ambassadors.

And more importantly, Mr. Secretary, if you could also touch upon and advise us as to how we can prevent this from happening again. . . .

A I would say with respect to the revelations that were brought out this morning, . . . that's not the way life is in Government as I have experienced it. . . .

Public service is a very rewarding and honorable thing, and nobody has to think they need to lie and cheat in order to be a public servant or to work in foreign policy. Quite to the contrary. If you are really going to be effective, . . . you have to be straightforward, and you have to conduct yourself in a basically honest way. . . .

I think there are a lot of things to be learned myself reflecting on these events, if not from these events, that seem to me . . . worth mentioning. . . . One that I think was most vivid in response to Senator [Sam] Nunn's [D.-Georgia] question, and that is I think the importance of separating the function of gathering and analyzing intelligence from the function of developing and carrying out policy. If the two things are mixed in together, it is too tempting to have your analysis and the selection of information that's presented favor the policy that you're advocating.

I believe that one of the reasons the President was given what I regard as wrong information, for example, about Iran and terrorism was that the agency, or the people

in the C.I.A., were too involved in this. So that's one point. And I feel very clear in my mind about this point.

And I know that long before this all emerged, I had come to have grave doubts about the objectivity and reliability of some of the intelligence I was getting. . . .

Mark A. Belnick, executive assistant to the chief counsel of the Senate committee. And did you begin developing the view, particularly as of Nov. 10, . . . that the President's advisers were misleading him and not giving him the facts concerning what had actually transpired in the Iran initiative?

A I developed a very clear opinion that the President was not being given accurate information, and I was very alarmed about it, and it became the preoccupying thing that I was working on through this period. And I felt that it was tremendously important for the President to get accurate information. . . . His judgment is excellent when he's given the right information, and he was not being given the right information.

And I felt as this went on that the people who were giving him the information . . . had a conflict of interest with the President. And they were trying to use his undoubted skills as a communicator to have him give a speech and give a press conference and say these things, and in doing so he would bail them out. . . . I don't want to try to attribute motives to other people too much, although I realize I am, but that's the way it shaped up to me. So I was in a battle to try to get what I saw as the facts to the President and get—and see that he understood them.

Now this was a very traumatic period for me because everybody was saying I'm disloyal to the President. I'm not speaking up for the policy. And I'm battling away here, and I could see people were calling for me to resign if I can't be loyal to the President, even including some of my friends and people who had held high office and should know that maybe there's more involved than they're seeing. And I frankly felt that I was the one who was loyal to the President, because I was the one who was trying to get him the facts so he could make a decision. And I must say, as he absorbed this, he did; he made the decision that we must get all these facts out. But it was a—it was a battle royal.

Q Mr. Secretary, in that battle royal to get out the facts, which you waged and which the record reflects that you waged, who was on the other side?

A Well, I can't say for sure, I—I feel that Admiral Poindexter was certainly on the other side of it. I felt that Director Casey was on the other side of it. And I don't know who all else, but they were the principals. . . .

Senator Inouye. Mr. Secretary, I have another question. And I ask this with great reluctance because I realize it is rather personal in nature, but I think it is relevant. . . . I've been advised that in August of 1986 you tendered a letter of resignation to the President of the United States. Is that true? And if so, can you tell us something about it?

A . . . That is true. And I have asked the President to let me leave this office on a couple of other occasions, earlier. . . .

Q Was that in any way related to the Iran-contra affair?

A Well, in August of 1986 I thought that it was over. . . . I didn't know anything about the contra side of it anyway. But on the effort with Iran, I thought it was basically on a proper track.

But it was because I felt a sense of estrangement. I knew the White House was very uncomfortable with me. I was very uncomfortable with what I was getting from the intelligence community, and I knew they were very uncomfortable with me—perhaps going back to the lie-detector test business. I could feel it.

What I have learned about the various things that were being done, I suppose explains why I was not in good odor with the N.S.C. staff and some of the others in the White House. I had a terrible time. There was a kind of guerrilla warfare going on, on all kinds of little things. For example, as you know, the Congress doesn't treat the State Department very well when it comes to appropriated funds. And not only have we historically taken a beating but we've been cut brutally . . . and I think in a manner that is not in the interests of the United States. . . .

But anyway, one of the conventions that's grown up—because we have no travel money to speak of . . .—the Air Force runs a White House Presidential Wing and when the Secretary of State has a mission, that gets approved and then I get an airplane and the airplane, it is paid for out of this budget. If I had to pay for that airplane, I couldn't travel. So you have me grounded unless I can get approved.

Now it's not a problem; the system works all right and it's just assumed that that's the way it's supposed to be. But I started having trouble because some people on the White House staff decided that they were going to make my life unhappy and they stopped approving these airplane things. And we fought about it and so on. And finally, I—I hated to do this. I went to the President and I gave him little memorandums to check off—yes, no. And that's no business for the Secretary of State to be taking up with the President of the United States.

But I found out there was a character in the White House that was in charge of doing this. His name was Jonathan Miller, and you've seen him here, and he was . . . trying to knock me out of trips. . . . But this was an atmosphere that I found—I felt that I was no longer on the wavelength that I should be on. And so I told the President, "I'd like to leave and here's my letter." And he stuck it in his drawer and he said, "You're tired. It's about time to go on vacation and let's talk about it after you get back from vacation." So I said, "O.K.," and I guess everybody knows what happened. In early—beginning early September last year, it was a tremendous stretch of activity and so nothing ever happened on that. . . .

At an earlier time, in the middle of 1983, I resigned. And that was because I discovered that Bud McFarlane, who was then the deputy national security adviser, was sent on a secret trip to the Middle East . . . without my knowledge, while we're busy negotiating out there. And also I found some things happened with respect to actions on Central America that I didn't know about beforehand.

So I went to the President and I said, "Mr. President, you don't need a guy like me for Secretary of State if this is the way things are going to be done, because when you send somebody out like that McFarlane trip, I'm done." In the labor relations business—I used to be Secretary of Labor and there used to be a lot of intervention in labor disputes and we used to say, "When the President hangs out his shingle, he'll get all the business." When—when the President hangs out his shingle and says, "You don't have to go through the State Department, just come right into the White House," he'll get all the business.

That's a big signal to countries out there about how to deal with the U.S.

Government. And it may have had had something to do with how events transpired, for all I know. But it's wrong; you can't do it that way. . . .

So the other time I resigned was after my big lie-detector test flap, and again I could see that I was on the outs with everybody and so I said, "Mr. President, why don't you let me go home. I like it in California." . . . And again, he wouldn't let that happen. And that was in late 1985. Mr. McFarlane had resigned, and Mr. McFarlane and I, I think, worked very effectively together in . . . our efforts with the U.S.S.R. and . . . in the end I didn't feel, with Mr. McFarlane having left, that it was fair to the President or the country for me to leave at the same time, so I didn't.

But I do think that in jobs like the job I have, where it is a real privilege to serve in this kind of job, or the others that you recounted, that you can't do the job well if you want it too much. You have to be willing to say goodbye, and I am.

Q I thank you very much, Mr. Secretary.

RECOMMENDATIONS ON ORGANIZING FOR NATIONAL SECURITY*

Tower Commission

In selection 28 (found in Part VIII of this text), weaknesses in the NSC as discovered by the Tower Commission were laid out. Presented here are the commission's recommendations for reform.

RECOMMENDATIONS

"Not only . . . is the Federal power over external affairs in origin and essential character different from that over internal affairs, but participation in the exercise of the power is significantly limited. In this vast external realm, with its important, complicated, delicate and manifold problems, the President alone has the power to speak or listen as a representative of the nation."
—United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936).

Whereas the ultimate power to formulate domestic policy resides in the Congress, the primary responsibility for the formulation and implementation of national security policy falls on the President.

It is the President who is the usual source of innovation and responsiveness in this field. The departments and agencies—the Defense Department, State Department, and CIA bureaucracies—tend to resist policy change. Each has its own perspective based on long experience. The challenge for the President is to bring his perspective to bear on these bureaucracies for they are his instruments for executing national security policy, and he must work through them. His task is to provide them leadership and direction.

The National Security Act of 1947 and the system that has grown up under it affords the President special tools for carrying out this important role. These tools are the National Security Council, the National Security Advisor, and the NSC staff. These are the means through which the creative impulses of the President are brought to bear on the permanent government. The National Security Act, and custom and practice, rightly give the President wide latitude in fashioning exactly how these means are used.

There is no magic formula which can be applied to the NSC structure and process to produce an optimal system. Because the system is the vehicle through which the President formulates and implements his national security policy, it must adapt to each individual President's style and management philosophy. This means that NSC structures and processes must be flexible, not rigid. Overprescription would . . . either destroy the system or render it ineffective.

Nevertheless, this does not mean there can be no guidelines or recommendations that might improve the operation of the system, whatever the particular style of the incumbent President. We have reviewed the operation of the system over the past 40 years, through good times and bad. We have listened carefully to the views of all the living former Presidents as well as those of most of the participants in their own national security systems.

---

* Reprinted from Report of the President's Special Review Board (the Tower Commission), Washington, D.C., February 26, 1987, pp. V-1–V-7.

With the strong caveat that flexibility and adaptability must be at the core, it is our judgment that the national security system seems to have worked best when it has in general operated along the lines set forth below.

Organizing for National Security Because of the wide latitude in the National Security Act, the President bears a special responsibility for the effective performance of the NSC system. A President must at the outset provide guidelines to the members of the National Security Council, his National Security Advisor, and the National Security Council staff. These guidelines, to be effective, must include how they will relate to one another, what procedures will be followed, what the President expects of them. If his advisors are not performing as he likes, only the President can intervene.

The National Security Council principals other than the President participate on the Council in a unique capacity.[1] Although holding a seat by virtue of their official positions in the Administration, when they sit as members of the Council they sit not as cabinet secretaries or department heads but as advisors to the President. They are there not simply to advance or defend the particular positions of the departments or agencies they head but to give their best advice to the President. Their job—and their challenge—is to see the issue from this perspective, not from the narrower interests of their respective bureaucracies.

The National Security Council is only advisory. It is the President alone who decides. When the NSC principals receive those decisions, they do so as heads of the appropriate departments or agencies. They are then responsible to see that the President's decisions are carried out by those organizations accurately and effectively.

This is an important point. The policy innovation and creativity of the President encounters a natural resistance from the executing departments. While this resistance is a source of frustration to every President, it is inherent in the design of the government. It is up to the politically appointed agency heads to ensure that the President's goals, designs, and policies are brought to bear on this permanent structure. Circumventing the departments, perhaps by using the National Security Advisor or the NSC staff to execute policy, robs the President of the experience and capacity resident in the departments. The President must act largely through them, but the agency heads must ensure that they execute the President's policies in an expeditious and effective manner. It is not just the obligation of the National Security Advisor to see that the national security process is used. All of the NSC principals—and particularly the President—have that obligation.

This tension between the President and the Executive Departments is worked out through the national security process described in the opening sections of this report. It is through this process that the nation obtains both the best of the creativity of the President and the learning and expertise of the national security departments and agencies.

This process is extremely important to the President. His decisions will benefit from the advice and perspective of all the concerned departments and agencies. History offers numerous examples of this truth. President Kennedy, for example, did not have adequate consultation before entering upon the Bay of Pigs invasion, one of his greatest failures. He remedied this in time for the Cuban missile crisis, one of his greatest successes. Process will not always produce brilliant ideas, but history suggests it can at least help prevent bad ideas from becoming Presidential policy.

The National Security Advisor It is the National Security Advisor who is primarily responsible for managing this process on a daily basis. The job requires skill, sensitivity,

and integrity. It is his responsibility to ensure that matters submitted for consideration by the Council cover the full range of issues on which review is required; that those issues are fully analyzed; that a full range of options is considered; that the prospects and risks of each are examined; that all relevant intelligence and other information is available to the principals; that legal considerations are addressed; that difficulties in implementation are confronted. Usually, this can best be accomplished through interagency participation in the analysis of the issue and a preparatory policy review at the Deputy or Under Secretary level.

The National Security Advisor assumes these responsibilities not only with respect to the President but with respect to all the NSC principals. He must keep them informed of the President's thinking and decisions. They should have adequate notice and an agenda for all meetings. Decision papers should, if at all possible, be provided in advance.

The National Security Advisor must also ensure that adequate records are kept of NSC consultations and Presidential decisions. This is essential to avoid confusion among Presidential advisors and departmental staffs about what was actually decided and what is wanted. Those records are also essential for conducting a periodic review of a policy or initiative, and to learn from the past.

It is the responsibility of the National Security Advisor to monitor policy implementation and to ensure that policies are executed in conformity with the intent of the President's decision. Monitoring includes initiating periodic reassessments of a policy or operation, especially when changed circumstances suggest that the policy or operation no longer serves U.S. interests.

But the National Security Advisor does not simply manage the national security process. He is himself an important source of advice on national security matters to the President. He is not the President's only source of advice, but he is perhaps the one most able to see things from the President's perspective. He is unburdened by departmental responsibilities. The President is his only master. His advice is confidential. He is not subject to Senate confirmation and traditionally does not formally appear before Congressional committees.

To serve the President well, the National Security Advisor should present his own views, but he must at the same time represent the views of others fully and faithfully to the President. The system will not work well if the National Security Advisor does not have the trust of the NSC principals. He, therefore, must not use his proximity to the President to manipulate the process so as to produce his own position. He should not interpose himself between the President and the NSC principals. He should not seek to exclude the NSC principals from the decision process. Performing both these roles well is an essential, if not easy, task.

In order for the National Security Advisor to serve the President adequately, he must have direct access to the President. Unless he knows first hand the views of the President and is known to reflect them in his management of the NSC system, he will be ineffective. He should not report to the President through some other official. While the Chief of Staff or others can usefully interject domestic political considerations into national security deliberations, they should do so as additional advisors to the President.

Ideally, the National Security Advisor should not have a high public profile. He should not try to compete with the Secretary of State or the Secretary of Defense as the articulator of public policy. They, along with the President, should be the spokesmen for the policies of the Administration. While a "passion for anonymity" is perhaps too strong a term, the National Security Advisor should generally operate offstage.

The NSC principals of course must have direct access to the President, with whatever frequency the President feels is appropriate. But these individual meetings should not be used by the principal to seek decisions or otherwise circumvent the system in the absence of the other principals. In the same way, the National Security Advisor should not use his scheduled intelligence or other daily briefings of the President as an opportunity to seek Presidential decision on significant issues.

If the system is to operate well, the National Security Advisor must promote cooperation rather than competition among himself and the other NSC principals. But the President is ultimately responsible for the operation of this system. If rancorous infighting develops among his principal national security functionaries, only he can deal with them. Public dispute over external policy by senior officials undermines the process of decision-making and narrows his options. It is the President's responsibility to ensure that it does not take place.

Finally, the National Security Advisor should focus on advice and management, not implementation and execution. Implementation is the responsibility and the strength of the departments and agencies. The National Security Advisor and the NSC staff generally do not have the depth of resources for the conduct of operations. In addition, when they take on implementation responsibilities, they risk compromising their objectivity. They can no longer act as impartial overseers of the implementation, ensuring that Presidential guidance is followed, that policies are kept under review, and that the results are serving the President's policy and the national interest.

The NSC Staff The NSC staff should be small, highly competent, and experienced in the making of public policy. Staff members should be drawn both from within and from outside government. Those from within government should come from the several departments and agencies concerned with national security matters. No particular department or agency should have a predominate role. A proper balance must be maintained between people from within and outside the government. Staff members should generally rotate with a stay of more than four years viewed as the exception.

A large number of staff action officers organized along essentially horizontal lines enhances the possibilities for poorly supervised and monitored activities by individual staff members. Such a system is made to order for energetic self-starters to take unauthorized initiatives. Clear vertical lines of control and authority, responsibility and accountability, are essential to good management.

One problem affecting the NSC staff is lack of institutional memory. This results from the understandable desire of a President to replace the staff in order to be sure it is responsive to him. Departments provide continuity that can help the Council, but the Council as an institution also needs some means to assure adequate records and memory. This was identified to the Board as a problem by many witnesses.

We recognize the problem and have identified a range of possibilities that a President might consider on this subject. One would be to create a small permanent executive secretariat. Another would be to have one person, the Executive Secretary, as a permanent position. Finally, a pattern of limited tenure and overlapping rotation could be used. Any of these would help reduce the problem of loss of institutional memory; none would be practical unless each succeeding President subscribed to it.

The guidelines for the role of the National Security Advisor also apply generally to the NSC staff. They should protect the process and thereby the President. Departments and

agencies should not be excluded from participation in that process. The staff should not be implementors or operators and staff should keep a low profile with the press.

PRINCIPAL RECOMMENDATION

The model we have outlined above for the National Security Council system constitutes our first and most important recommendation. It includes guidelines that address virtually all of the deficiencies in procedure and practice that the Board encountered in the Iran/Contra affair as well as in other case studies of this and previous administrations.

We believe this model can enhance the performance of a President and his administration in the area of national security. It responds directly to President Reagan's mandate to describe the NSC system as it ought to be.

The Board recommends that the proposed model be used by Presidents in their management of the national security system.

SPECIFIC RECOMMENDATIONS

In addition to its principal recommendation regarding the organization and functioning of the NSC system and roles to be played by the participants, the Board has a number of specific recommendations.

1. The National Security Act of 1947 The flaws of procedure and failures of responsibility revealed by our study do not suggest any inadequacies in the provisions of the National Security Act of 1947 that deal with the structure and operation of the NSC system. Forty years of experience under that Act demonstrate to the Board that it remains a fundamentally sound framework for national security decision-making. It strikes a balance between formal structure and flexibility adequate to permit each President to tailor the system to fit his needs.

As a general matter, the NSC staff should not engage in the implementation of policy or the conduct of operations. This compromises their oversight role and usurps the responsibilities of the departments and agencies. But the inflexibility of a legislative restriction should be avoided. Terms such as "operation" and "implementation" are difficult to define, and a legislative proscription might preclude some future President from making a very constructive use of the NSC staff.

Predisposition on sizing of the staff should be toward fewer rather than more. But a legislative restriction cannot foresee the requirements of future Presidents. Size is best left to the discretion of the President, with the admonition that the role of the NSC staff is to review, not to duplicate or replace, the work of the departments and agencies.

We recommend that no substantive change be made in the provisions of the National Security Act dealing with the structure and operation of the NSC system.

2. Senate Confirmation of the National Security Advisor It has been suggested that the job of the National Security Advisor has become so important that its holder should be screened by the process of confirmation, and that once confirmed he should return frequently for questioning by the Congress. It is argued that this would improve the accountability of the National Security Advisor.

We hold a different view. The National Security Advisor does, and should continue, to serve only one master, and that is the President. Further, confirmation is inconsistent with the role the National Security Advisor should play. He should not decide, only advise. He should not engage in policy implementation or operations. He should serve the President, with no collateral and potentially diverting loyalties.

Confirmation would tend to institutionalize the natural tension that exists between the Secretary of State and the National Security Advisor. Questions would increasingly arise about who really speaks for the President in national security matters. Foreign governments could be confused or would be encouraged to engage in "forum shopping."

Only one of the former government officials interviewed favored Senate confirmation of the National Security Advisor. While consultation with Congress received wide support, confirmation and formal questioning were opposed. Several suggested that if the National Security Advisor were to become a position subject to confirmation, it could induce the President to turn to other internal staff or to people outside government to play that role.

We urge the Congress not to require Senate confirmation of the National Security Advisor.

3. The Interagency Process It is the National Security Advisor who has the greatest interest in making the national security process work, for it is this process by which the President obtains the information, background, and analysis he requires to make decisions and build support for his program. Most Presidents have set up interagency committees at both a staff and policy level to surface issues, develop options, and clarify choices. There has typically been a struggle for the chairmanships of these groups between the National Security Advisor and the NSC staff on the one hand, and the cabinet secretaries and department officials on the other.

Our review of the operation of the present system and that of other administrations where committee chairmen came from the departments has led us to the conclusion that the system generally operates better when the committees are chaired by the individual with the greatest stake in making the NSC system work.

We recommend that the National Security Advisor chair the senior-level committees of the NSC system.

4. Covert Actions Policy formulation and implementation are usually managed by a team of experts led by policymaking generalists. Covert action requirements are no different, but there is a need to limit, sometimes severely, the number of individuals involved. The lives of many people may be at stake, as was the case in the attempt to rescue the hostages in Tehran. Premature disclosure might kill the idea in embryo, as could have been the case in the opening of relations with China. In such cases, there is a tendency to limit those involved to a small number of top officials. This practice tends to limit severely the expertise brought to bear on the problem and should be used very sparingly indeed.

The obsession with secrecy and preoccupation with leaks threaten to paralyze the government in its handling of covert operations. Unfortunately, the concern is not misplaced. The selective leak has become a principal means of waging bureaucratic warfare. Opponents of an operation kill it with a leak; supporters seek to build support through the same means.

We have witnessed over the past years a significant deterioration in the integrity of process. Rather than a means to obtain results more satisfactory than the position of any of

the individual departments, it has frequently become something to be manipulated to reach a specific outcome. The leak becomes a primary instrument in that process.

This practice is destructive of orderly governance. It can only be reversed if the most senior officials take the lead. If senior decision-makers set a clear example and demand compliance, subordinates are more likely to conform.

Most recent administrations have had carefully drawn procedures for the consideration of covert activities. The Reagan Administration established such procedures in January, 1985, then promptly ignored them in their consideration of the Iran initiative.

We recommend that each administration formulate precise procedures for restricted consideration of covert action and that, once formulated, those procedures be strictly adhered to.

5. The Role of the CIA Some aspects of the Iran arms sales raised broader questions in the minds of members of the Board regarding the role of the CIA. The first deals with intelligence.

The NSC staff was actively involved in the preparation of the May 20, 1985, update to the Special National Intelligence Estimate on Iran. It is a matter for concern if this involvement and the strong views of NSC staff members were allowed to influence the intelligence judgments contained in the update. It is also of concern that the update contained the hint that the United States should change its existing policy and encourage its allies to provide arms to Iran. It is critical that the line between intelligence and advocacy of a particular policy be preserved if intelligence is to retain its integrity and perform its proper function. In this instance, the CIA came close enough to the line to warrant concern.

We emphasize to both the intelligence community and policymakers the importance of maintaining the integrity and objectivity of the intelligence process.

6. Legal Counsel From time to time issues with important legal ramifications will come before the National Security Council. The Attorney General is currently a member of the Council by invitation and should be in a position to provide legal advice to the Council and the President. It is important that the Attorney General and his department be available to interagency deliberations.

The Justice Department, however, should not replace the role of counsel in the other departments. As the principal counsel on foreign affairs, the Legal Adviser to the Secretary of State should also be available to all the NSC participants.

Of all the NSC participants, it is the Assistant for National Security Affairs who seems to have had the least access to expert counsel familiar with his activities.

The Board recommends that the position of Legal Adviser to the NSC be enhanced in stature and in its role within the NSC staff.

7. Secrecy and Congress There is a natural tension between the desire for secrecy and the need to consult Congress on covert actions. Presidents seem to become increasingly concerned about leaks of classified information as their administrations progress. They blame Congress disproportionately. Various cabinet officials from prior administrations indicated to the Board that they believe Congress bears no more blame than the Executive Branch.

However, the number of Members and staff involved in reviewing covert activities is large; it provides cause for concern and a convenient excuse for Presidents to avoid Congressional consultation.

We recommend that Congress consider replacing the existing Intelligence Committees of the respective Houses with a new joint committee with a restricted staff to oversee the intelligence community, patterned after the Joint Committee on Atomic Energy that existed until the mid-1970s.

8. Privatizing National Security Policy Careful and limited use of people outside the U.S. Government may be very helpful in some unique cases. But this practice raises substantial questions. It can create conflict of interest problems. Private or foreign sources may have different policy interests or personal motives and may exploit their association with a U.S. government effort. Such involvement gives private and foreign sources potentially powerful leverage in the form of demands for return favors or even blackmail.

The U.S. has enormous resources invested in agencies and departments in order to conduct the government's business. In all but a very few cases, these can perform the functions needed. If not, then inquiry is required to find out why.

We recommend against having implementation and policy oversight dominated by intermediaries. We do not recommend barring limited use of private individuals to assist in United States diplomatic initiatives or in covert activities. We caution against use of such people except in very limited ways and under close observation and supervision.

EPILOGUE

If but one of the major policy mistakes we examined had been avoided, the nation's history would bear one less scar, one less embarrassment, one less opportunity for opponents to reverse the principles this nation seeks to preserve and advance in the world.

As a collection, these recommendations are offered to those who will find themselves in situations similar to the ones we reviewed; under stress, with high stakes, given little time, using incomplete information, and troubled by premature disclosure. In such a state, modest improvements may yield surprising gains. This is our hope.

NOTE

1. As discussed in more detail in Part II [not reprinted in this text] the statutory members of the National Security Council are the President, Vice President, Secretary of State, and Secretary of Defense. By the phrase "National Security Council principals" or "NSC principals," the Board generally means those four statutory members plus the Director of Central Intelligence and the Chairman of the Joint Chiefs of Staff.

GLOSSARY

ACCM	Alternative or Compensatory Control Measure
AFIO	Association of Former Intelligence Officers
AG	Attorney General
Aman	Agaf ha-Modi'in (Israeli military intelligence)
ANC	African National Congress
BDA	Battle Damage Assessment
BfV	Bundesamt für Verfassungsschutz (German equivalent of the FBI)
BMD	Ballistic Missile Defense
BND	Bundesnachrichtendienst (German foreign intelligence service)
BSO	Black September Organization
BW	Biological Weapons
CA	Covert Action
CAS	Covert Action Staff (CIA)
CBW	Chemical/Biological Warfare
CCP	Consolidated Cryptographic Program
CDA	Congressionally Directed Action
CE	Counterespionage
CHAOS	Code name for CIA illegal domestic spying
CI	Counterintelligence
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CIG	Central Intelligence Group
CMS	Community Management Staff
CNC	Crime and Narcotics Center (CIA)

COINTELPRO	FBI Counterintelligence Program
COMINT	Communications Intelligence
Corona	Codename for first U.S. spy satellite system
COS	Chief of Station (CIA)
COSPO	Community Open Source Program Office
CPA	Covert Political Action
CPSU	Communist Party of the Soviet Union
CSI	Committee on Intelligence Services (Britain)
CT	Counterterrorism
CTC	Counterterrorism Center (CIA)
CW	Chemical Weapons
D & D	Denial and Deception
DARP	Defense Airborne Reconnaissance Program
DAS	Deputy Assistant Secretary
DBA	Dominant Battlefield Awareness
DC	Deputies Committee (NSC)
DCD	Domestic Contact Division (CIA)
DCI	Director of Central Intelligence
D/CIA	Director of Central Intelligence Agency
DDA	Deputy Director of Administration (CIA)
DDCI	Deputy Director for Central Intelligence (DDCI)
DD/CIA	Deputy Director, Central Intelligence Agency
DDO	Deputy Director for Operations (CIA)
DDP	Deputy Director for Plans (CIA)
DDS&T	Deputy Director for Science and Technology (CIA)
DEA	Drug Enforcement Administration
DGSE	Directorie Génerale de la Sécurité Extérieure (French intelligence service)
DHS	Department of Homeland Security
DI	Directorate of Intelligence (CIA)
DIA	Defense Intelligence Agency
DIA/Humint	Defense Humint Service
DINSUM	*Defense Intelligence Summary*
DNI	Director of National Intelligence
DO	Directorate of Operations
DoD	Department of Defense
DOD	Domestic Operations Division (CIA)
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Treasury
DOS	Department of State
DP	Directorate of Plans (CIA)
DST	Directoire de Surveillance Territore (France)
ECHR	European Convention of Human Rights

ELINT	Electronic Intelligence
ENIGMA	Code machine used by the Germans during World War II
EO	Executive Order
EOP	Executive Office of the President
ETF	Environmental Task Force (CIA)
FARC	Fuerzas Armadas Revolucionarias in Colombia
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FISA	Foreign Intelligence Surveillance Act (1978)
FNLA	National Front for the Liberation of Angola
FOIA	Freedom of Information Act
FRD	Foreign Resources Division (CIA)
FSB	Federal'naya Sluzba Besnopasnoti (Federal Security Service, Russia)
GAO	General Accountability Office (Congress)
GCHQ	Government Communications Headquarters (the British NSA)
GEO	Geosynchronous Orbit
GEOINT	Geospatial Intelligence
GRU	Soviet Military Intelligence
GSG	German Counterterrorism Service
HEO	High Elliptical Orbit
HPSCI	House Permanent Select Committee on Intelligence
HUAC	House Un-American Activities Committee
HUMINT	Human Intelligence (assets)
I & W	Indicators and Warning
IAEA	International Atomic Energy Agency
IAF	Israel Air Force
IC	Intelligence Community
ICS	Intelligence Community Staff
IDF	Israeli Defense Force
IG	Inspector General
IMINT	Imagery Intelligence (photographs)
INR	Bureau of Intelligence and Research (Department of State)
INTELINK	An intelligence community computer information system
INTs	Collection disciplines (IMINT, SIGINT, OSINT, HUMINT, MASINT)
IOB	Intelligence Oversight Board (White House)
ISA	Israeli Security Agency
ISC	Intelligence and Security Committee (U.K.)
ISI	Inter-Services Intelligence (Pakistani intelligence agency)
IT	Information Technology
JCAE	Joint Committee on Atomic Energy
JCS	Joint Chiefs of Staff
JIC	Joint Intelligence Committee (U.K.)

JSOC	Joint Special Operations Command
JSTARS	Joint Surveillance Target Attack Radar Systems
KGB	Soviet Secret Police
KH	Keyhole (satellite)
LTTE	Tamil Tigers of Tamil Elam
MAGIC	Allied code-breaking operations against the Japanese in the World War II
MASINT	Measurement and Signatures Intelligence
MI5	Security Service (U.K.)
MI6	Secret Intelligence Service (U.K.)
MON	Memoranda of Notification
MONGOOSE	Code name for CIA covert actions against Fidel Castro of Cuba (1961–62)
Mossad	Israeli Intelligence Service
MPLA	Popular Movement for the Liberation of Angola
NAACP	National Association for the Advancement of Colored People
NBC	Nuclear, Biological, and Chemical (Weapons)
NCS	National Clandestine Service
NCIC	National Counterintelligence Center
NCTC	National Counterterrorism Center
NED	National Endowment for Democracy
NFIB	National Foreign Intelligence Board
NFIC	National Foreign Intelligence Council
NFIP	National Foreign Intelligence Program
NGA	National Geospatial-Intelligence Agency
NGO	Nongovernmental organization
NIA	National Intelligence Authority
NIC	National Intelligence Council
NID	*National Intelligence Daily*
NIE	National Intelligence Estimate
NIO	National Intelligence Officer
NOC	Nonofficial Cover
NPIC	National Photographic Interpretation Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council (White House)
NSCID	National Security Council Intelligence Directive
NTM	National Technical Means
OB	Order of Battle
OC	Official Cover
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
ONI	Office of Naval Intelligence

OPC	Office of Policy Coordination
OSD	Office of the Secretary of Defense
OSINT	Open-Source Intelligence
OSS	Office of Strategic Services
P & E	Processing and Exploitation
PDB	*President's Daily Brief*
PFIAB	President's Foreign Intelligence Advisory Board (White House)
PFLP	Popular Front for the Liberation of Palestine
PIJ	Palestinian Islamic Jihad
PLO	Palestine Liberation Organization
PM	Paramilitary
PRO	Public Record Office (U.K.)
RADINT	Radar Intelligence
RFE	Radio Free Europe
RL	Radio Liberty
SA	Special Activities Division (DO/CIA)
SAS	Special Air Service (U.K.)
SBS	Special Boat Service (U.K.)
SDO	Support to Diplomatic Operations
SHAMROCK	Code name for illegal NSA interception of cables
SIG	Senior Interagency Group
SIGINT	Signals Intelligence
SIS	Secret Intelligence Service (U.K., also known as MI6)
SISDE	Italian Intelligence Service
SMO	Support to Military Operations
SMS	Secretary's *Morning Summary* (Department of State)
SNIE	Special National Intelligence Estimate
SO	Special Operations (CIA)
SOCOM	Special Operations Command (Department of Defense)
SOE	Special Operations Executive (U.K.)
SOG	Special Operations Group (DO/CIA)
SOVA	Office of Soviet Analysis (CIA)
SSCI	Senate Select Committee on Intelligence
SVR	Russian Foreign Intelligence Service
TECHINT	Technical Intelligence
TELINT	Telemetery Intelligence
TIARA	Tactical Intelligence and Related Activities
TPED	Tasking, Processing, Exploitation, and Dissemination
UAV	Unmanned Aerial Vehicle (drone)
ULTRA	Code name for the Allied operation that deciphered the German ENIGMA code in World War II
UN	United Nations
UNITA	National Union for the Total Independence of Angola

UNSCOM	United Nations Special Commission
USIB	United States Intelligence Board
USTR	United States Trade Representative
VCI	Viet Cong Infrastructure
VENONA	Code name for SIGINT intercepts against Soviet spying in America
VOA	Voice of America
VX	A deadly nerve agent used in chemical weapons
WMD	Weapons of mass destruction

INDEX

ABOUT THE EDITOR AND CONTRIBUTORS

EDITOR

Loch K. Johnson is Regents Professor of Public and International Affairs at the University of Georgia and author of several books and over 100 articles on U.S. intelligence and national security. His books include *The Making of International Agreements* (1984); *A Season of Inquiry* (1985); *Through the Straits of Armageddon* (1987, coedited with Paul Diehl); *Decisions of the Highest Order* (1988, coedited with Karl F. Inderfurth); *America's Secret Power* (1989); *Runoff Elections in the United States* (1993, coauthored with Charles S. Bullock III); *America as a World Power* (1995); *Secret Agencies* (1996); *Bombs, Bugs, Drugs, and Thugs* (2000); *Fateful Decisions* (2004, coedited with Karl F. Inderfurth); *Strategic Intelligence* (2004, coedited with James J. Wirtz); *Who's Watching the Spies?* (2005, coauthored with Hans Born and Ian Leigh); *American Foreign Policy* (2005, coauthored with Daniel Papp and John Endicott); and *Seven Sins of American Foreign* Policy (2007). He has served as special assistant to the chair of the Senate Select Committee on Intelligence (1975–76), staff director of the House Subcommittee on Intelligence Oversight (1977–79), and special assistant to the chair of the Aspin-Brown Commission on Intelligence (1995–96). In 1969–70, he was an American Political Science Association Congressional Fellow. He has served as secretary of the American Political Science Association and President of the International Studies Association, South. Born in New Zealand and educated at the University of California, Johnson has taught at the University of Georgia since 1979, winning its Meigs Professorship for meritorious teaching and its Owens Award for outstanding accomplishments in the field of social science research. In 2000, he led the founding of the School of Public and

International Affairs at the University of Georgia. He is the senior editor of the international journal *Intelligence and National Security*.

CONTRIBUTORS

Matthew M. Aid is Managing Director in the Washington, DC, office of Citigate Global Intelligence and Security and coeditor of *Secrets of Signals Intelligence During the Cold War and Beyond* (2001).

James E. Baker sits on the U.S. Court of Appeals for the Armed Forces. He previously served as Special Assistant to the President and Legal Adviser to the National Security Council and as Deputy Legal Adviser to the NSC. He has also served as Counsel to the President's Foreign Intelligence Advisory Board, an attorney at the Department of State, a legislative aide to Senator Daniel Patrick Moynihan, and as a Marine Corps infantry officer. He is the coauthor with Michael Reisman of *Regulating Covert Action* (Yale University Press, 1992).

David M. Barrett is Associate Professor of Political Science at Villanova University and author of *Congress and the CIA* (Kansas, 2005).

Hans Born is a senior fellow in democratic governance of the security sector at the Geneva Centre for Democratic Control of the Armed Forces (DCAF). He is an external member of the crisis management and security policy faculty of the Federal Institute of Technology and a guest lecturer on governing nuclear weapons at the UN Disarmament Fellowship Programme. He has written, co-authored, and co-edited various books on international relations and security policy, including the Inter-Parliamentary Union Handbook on *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices* (Geneva: IPU/DCAF, 2003, translated in 30 languages); *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005, translated in 10 languages); *Who is Watching the Spies? Establishing Intelligence Agency Accountability* (Dulles, VA: Potomac Publishers, 2005); *Civil-Military Relations in Europe: Learning from Crisis and Institutional Change* (London: Routledge, 2006); and *The Double Democratic Deficit: Parliamentary Accountability and the Use of Force under International Auspices* (London: Ashgate Publishers: Aldershot).

A. Denis Clift is President of the Department of Defense Joint Military Intelligence College. He was born in New York City and educated at Friends Seminary, Phillips Exeter Academy (1954), Stanford University (B.A., 1958), and the London School of Economics and Political Science (M.Sc., 1967). He began a career of public service as a naval officer in the Eisenhower and Kennedy administrations and has served in military and civilian capacities in ten administrations, including thirteen successive years in the Executive Office of the President and the White House. From 1971–76, he served on the National Security

Council staff. From 1974–76, he was head of President Ford's National Security Council staff for the Soviet Union and Eastern and Western Europe. From 1977–81, he was Assistant for National Security Affairs to the Vice President. From 1991–94, he was Chief of Staff, Defense Intelligence Agency. From 1963–66, he was the editor of the U.S. Naval Institute *Proceedings*. His published fiction and nonfiction include the novel *A Death in Geneva* (Ballantine Books, Random House), *Our World in Antarctica* (Rand McNally), *With Presidents to the Summit* (George Mason University Press), and *Clift Notes: Intelligence and the Nation's Security* (JMIC Writing Center Press).

William J. Daugherty holds a doctorate in government from the Claremont Graduate School and is Associate Professor of government at Armstrong Atlantic State University in Savannah, Georgia. A retired senior officer in the CIA, he is also the author of *In the Shadow of the Ayatollah: A CIA Hostage in Iran* (Annapolis, 2001) and *Executive Secrets: Covert Action and the Presidency* (Kentucky, 2004).

Jack Davis served in the CIA from 1956 to 1990 as analyst, manager, and teacher of analysts. He now is an independent contractor with the Agency, specializing in analytic methodology. He is a frequent contributor to the journal *Studies in Intelligence*.

Stuart Farson is Lecturer, Political Science Department, Simon Fraser University, Vancouver/Surrey, Canada. He is a former Secretary-Treasurer of the Canadian Association for Security and Intelligence Studies, and served as Director of Research for the Special Committee of the House Commons (Canada) on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act. He has numerous articles on security, intelligence, and policing issues and is the coeditor of *Security and Intelligence in a Changing World* (with David Stafford and Wesley K. Wark, Cass, 1991).

Timothy Gibbs is a final-year doctoral student in history at Robinson College, Cambridge University, and a member of the Cambridge University Intelligence Seminar. He is also a former Visiting Scholar at the University of Georgia. His doctoral dissertation, titled *British and American Intelligence and the Atom Spies*, was submitted in the summer of 2006 and was supervised by Professor Christopher Andrew.

Peter Gill is Reader in Politics and Security, Liverpool John Moores University, Liverpool, United Kingdom. He is coauthor of *Introduction to Politics* (1988, 2nd ed.) and *Intelligence in an Insecure World* (2006). He is currently researching the control and oversight of domestic security in intelligence agencies.

Harold M. Greenberg graduated with a B.A. in history from Yale University in 2005. At Yale, he participated in the Studies in Grand Strategy program, and he has recently published research on CIA covert action in the 1950s. He now works as a legislative aide in the U.S. House of Representatives.

Daniel S. Gressang IV is Professor at the Joint Military Intelligence College (JMIC) in Washington, DC, and serves concurrently as the National Security Agency/National Cryptologic School of Liaison to JMIC. He has researched, written, and lectured extensively on terrorism and counterinsurgency. His research focuses primarily on the application of complex adaptive systems perspectives to understanding the dynamics of terror and other forms of unconventional warfare. In 2004, he was designated Intelligence Community Officer by the Director of Central Intelligence.

Glenn Hastedt received his doctorate in political science from Indiana University. Until recently he was Professor and Chair of the Political Science Department at James Madison University. He is now chair of the Justice Studies Department there. Among his publications is *American Foreign Policy: Past, Present, Future*, 6th ed. (Prentice Hall).

John Hollister Hedley, during more than thirty years at CIA, edited the *President's Daily Brief*, briefed the *PDB* at the White House, served as Managing Editor of the *National Intelligence Daily*, and was Chairman of the CIA's Publications Review Board. Now retired, Hedley has taught intelligence at Georgetown University and serves as a consultant to the National Intelligence Council and the Center for the Study of Intelligence.

Michael Herman served from 1952 to 1987 in Britain's Government Communications Headquarters, with secondments to the Cabinet Office and the Ministry of Defence. Since retirement he has written extensively on intelligence matters, with official clearance. He has had academic affiliations with Nuffield and St. Antony's Colleges in Oxford and is Founder Director of the Oxford Intelligence Group and Honorary Departmental Fellow at Aberystwyth University. In 2005 he received the degree of Honorary D.Litt from Nottingham University. He is a leading British intelligence scholar and author of *Intelligence Power in Peace and War* (Cambridge, 2001).

Frederick P. Hitz is Lecturer (Diplomat in Residence) in Public and International Affairs, Woodrow Wilson School, Princeton University.

Max M. Holland is the author of *The Kennedy Assassination Tapes* (Knopf, 2004).

Arthur S. Hulnick is Associate Professor of International Relations at Boston University. He is a veteran of thirty-five years of intelligence service, including seven years in Air Force Intelligence and twenty-eight years in the CIA. He is author of *Fixing the Spy Machine* (Praeger, 1999) and *Keeping Us Safe* (Praeger, 2004).

Rhodri Jeffreys-Jones is Professor of American History at the University of Edinburgh. The author of several books on intelligence history, he is currently completing a study of the FBI.

Ephraim Kahana is Professor of Political Science and faculty member in the Western Galilee College, Acre, Israel. He teaches courses on international relations, national security and intelligence, and foreign policy in the National Security Program in the University of Haifa. Kahana has written numerous papers on intelligence and foreign policy. His most recent book is the *Historical Dictionary of Israeli Intelligence* (2006).

Patrick Radden Keefe is a graduate of the School of Law at Yale University and is presently a Fellow with the Century Foundation in New York City. He is the author of *Chatter: Uncovering the Echelon Surveillance Network and the Secret World of Global Eavesdropping* (Random House, 2006), and has published essays in *The New York Review of Books*, *The New York Times Magazine*, the *New York Times*, the *Boston Globe*, the *Yale Journal of International Law*, *Legal Affairs*, *Slate*, and *Wired*. He has been a Marshall Scholar and a 2003 fellow at the Dorothy and Lewis B. Cullman Center for Scholars and Writers at the New York Public Library.

Jennifer D. Kibbe is Assistant Professor of Government at Franklin and Marshall College. Between 2002 and 2004, she was a postdoctoral fellow at the Brookings Institution. Her research interests include U.S. foreign policy, intelligence and covert action, presidential decision making, and political psychology. She has published work on U.S. policy in Iraq and the Middle East, and the military's involvement in covert actions.

Katharina von Knop is a doctoral candidate in Political Science at Leopold-Franzens University in Innsbruck, Austria, specializing in counter- and antiterrorism, and coeditor with Heinrich Neisser and Martin van Creveld of *Countering Modern Terrorism: History, Current Issues, and Future Threats* (2005).

Lawrence J. Lamanna is a doctoral candidate in the School of Public and International Affairs at the University of Georgia. He holds an M.A. from Yale University and a B.A. from the University of Notre Dame.

Ian Leigh is Professor of Law and Codirector of the Human Rights Centre at the University of Durham. He lives in Durham, England.

Kristin M. Lord is Associate Dean at George Washington University's Elliott School of International Affairs. In 2005–2006, she was a Council on Foreign Relations International Affairs Fellow and Special Adviser to the Under Secretary of State for Democracy and Global Affairs. Lord is the author of *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security Democracy or Peace* (SUNY Press, 2006); coeditor, with Bernard I. Finel, of *Power and Conflict in the Age of Transparency* (Palgrave Macmillan, 2000); and the author of numerous book chapters, articles, and papers on international politics and security. Lord received her doctorate in government from Georgetown University.

Minh A. Luong is Assistant Director of International Security Studies at Yale University, where he teaches in the Department of History. He also serves as adjunct Assistant Professor of Public Policy at the Taubman Center at Brown University.

Cynthia M. Nolan earned a doctorate at American University in the School of International Service, researching intelligence oversight. She is a former officer in the Directorate of Operations in the CIA and has published in the *International Journal of Intelligence and Counterintelligence*.

Kevin A. O'Brien is a former research associate with the Canadian Institute of Strategic Studies and is currently a senior analyst for RAND Europe.

Mark Phythian is Professor of International Security and Director of the History and Governance Research Institute at the University of Wolverhampton, United Kingdom. He is the author of *Intelligence in an Insecure World* (2006, with Peter Gill), *The Politics of British Arms Sales Since 1964* (2000), and *Arming Iraq* (1997), as well as numerous journal articles on intelligence and security issues.

Harry Howe Ransom is Professor Emeritus of Political Science at Vanderbilt University. He has a B.A. from Vanderbilt and an M.A. and Ph.D. from Princeton University. He was a Congressional Fellow of the American Political Science Association and a Fellow of the Woodrow Wilson International Center for Scholars. He taught at Princeton, Vassar College, Michigan State University, Harvard University, and the University of Leeds. His books include *Central Intelligence and National Security* (1958), *Can American Democracy Survive Cold War?* (1963), and *The Intelligence Establishment* (1970).

Jeffrey T. Richelson is Senior Fellow with the National Security Archive in Washington, DC, and author of *The Wizards of Langley*, *The U.S. Intelligence Community*, *A Century of Spies*, and *America's Eyes in Space*, as well as numerous articles on intelligence activities. He received his doctorate in political science from the University of Rochester and has taught at the University of Texas, Austin, and the American University, Washington, DC. He lives in Los Angeles.

Jerel A. Rosati is Professor of Political Science and International Studies at the University of South Carolina since 1982. His area of specialization is the theory and practice of foreign policy, focusing on the U.S. policy-making process, decision-making theory, and the political psychological study of human cognition. He is the author and editor of five books and over forty articles and chapters. He has received numerous outstanding teaching awards. He has been Visiting Professor at Somalia National University in Mogadishu and Visiting Scholar at China's Foreign Affairs College in Beijing. He also has been a Research Associate in the Foreign Affairs and National Defense Division of the Library of Congress's Congressional Research Service, President of the International

Studies Association's Foreign Policy Analysis Section, and President of the Southern region of the International Studies Association.

Richard L. Russell is Professor of national security studies at the National Defense University. He is also an adjunct associate professor in the Security Studies Program and research associate in the Institute for the Study of Diplomacy at Georgetown University. He previously served as a CIA political-military analyst. Russell is the author of *Weapons Proliferation and War in the Greater Middle East: Strategic Contest* (2005).

Frederick A. O. Schwarz Jr. received an A.B. from Harvard University and J.D. from Harvard Law School, where he was an editor of the *Law Review*. After a year's clerkship with Hon. J. Edward Lumbard, U.S. Court of Appeals for the Second Circuit, he worked one year for the Nigerian government as Assistant Commissioner for Law Revision under a Ford Foundation grant. He joined the New York City law firm of Cravath, Swaine and Moore in 1963 and was elected a partner in 1969. From 1975 through mid-1976, he served as Chief Counsel to the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the Church Committee); from 1982–89, he served as Corporation Counsel and head of the Law Department of the City of New York. In 1989, he chaired the New York City Charter Revision Commission.

James M. Scott is Professor and Chair of the Department of Political Science at Oklahoma State University. His areas of specialization include foreign policy analysis and international relations, with particular emphasis on U.S. foreign policy making and the domestic sources of foreign policy. He is author or editor of four books, over forty articles, book chapters, review essays, and other publications. He has been President of the Foreign Policy Analysis section and President of the Midwest region of the International Studies Association, where he has also served as conference organizer for both sections and has been a two-time winner of the Klingberg Award for Outstanding Faculty Paper at the ISA Midwest Annual Meeting. Since 1996, he has received over two dozen awards from students and peers for his outstanding teaching and research, including his institution's highest awards for scholarship in 2000 and 2001. Since 2005, he has been Director of the Democracy and World Politics Summer Research Program, a National Science Foundation Research Experience for Undergraduates.

Len Scott is Professor of International Politics at the University of Wales, Aberystwyth, where he is Director of the Centre for Intelligence and International Security Studies. Among his recent publications are *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows* (2004, coedited with Peter Jackson) and *Planning Armageddon: Britain, the United States and the Command of Nuclear Forces, 1943–1964* (2000, coedited with Stephen Twigge).

Katherine A. S. Sibley is Professor and Chair of the History Department at St. Joseph's University. She is currently working on a biography of Florence Kling

Harding, titled *America's First Feminist First Lady*. Sibley's work will revise the typical portrait of Mrs. Harding as manipulative, unhappy wife, casting new light on her public and private life. In 2004, Sibley published *Red Spies in America: Stolen Secrets and the Dawn of the Cold War* with the University Press of Kansas. She is also the author of *The Cold War* (1998) and *Loans and Legitimacy: The Evolution of Soviet-American Relations, 1919–1933* (1996). Her work has appeared in journals including *American Communist History*, *Peace and Change*, and *Diplomatic History*, and she also serves as book review editor for *Intelligence and National Security*. She is a three-term Commonwealth Speaker for the Pennsylvania Humanities Council.

Jennifer Sims is Director of Intelligence Studies and Visiting Professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service. She also consults for the U.S. government and private sector on homeland security and intelligence related matters. Prior to this, Sims was Research Professor at Johns Hopkins University's Nitze School of Advanced International Studies in Washington, DC (Fall 2001–Summer 2003). She has served as defense and foreign policy adviser to Senator John Danforth (1990–94), a professional staff member of the Senate Select Committee on Intelligence (1991–94), Deputy Assistant Secretary of State for Intelligence Coordination (1994–98), and as the Department of State's first Coordinator for Intelligence Resources and Planning in the office of the Under Secretary for Management. In 1998 Sims was awarded the U.S. Intelligence Community's Distinguished Service Medal. She received her B.A. degree from Oberlin College and her M.A. and Ph.D. in national security studies from Johns Hopkins University in 1978 and 1985, respectively. She is the author of a number of books and articles on intelligence and arms control. The most recent of these include "Foreign Intelligence Liaison: Devils, Deals and Details," *International Journal of Intelligence and Counterintelligence Affairs* (Summer 2006); *Transforming US Intelligence,* coedited with Burton Gerber (Georgetown University Press, 2005); "Transforming U.S. Espionage: A Contrarian's Approach," *Georgetown Journal of International Affairs* (Winter/Spring 2005); "Domestic Factors in Arms Control: The U.S. Case," in Jeffrey A Larson (ed.), *Arms Control: Cooperative Security in a Changing Environment* (Lynne Rienner, 2002); "What Is Intelligence? Information for Decision-Makers," in Roy Godson, Ernest R. May, and Gary Schmitt, *U.S. Intelligence at the Crossroads* (Brassey's, 1995); "The Cambridge Approach Reconsidered," *Daedalus* 120 (Winter 1991); and *Icarus Restrained: An Intellectual History of American Arms Control* (Westview Press, 1990).

Robert David Steele is CEO of OSS.Net, an international open source intelligence provider. As the son of an oilman, a Marine Corps infantry officer, and a clandestine intelligence case officer for the CIA, he has spent over twenty years abroad in Asia and Central and South America. As a civilian intelligence officer he spent three back-to-back tours overseas, including one tour as one of the first officers assigned full-time to terrorism, and three headquarters tours in offensive

counterintelligence, advanced information technology, and satellite program management. He resigned from the CIA in 1988 to be the senior civilian founder of the Marine Corps Intelligence Command. He resigned from the Marines in 1993. He is the author of three works on intelligence, as well as the editor of a book on peacekeeping intelligence. He has earned graduate degrees in international relations and public administration, is a graduate of the Naval War College, and has a certificate in Intelligence Policy. He is also a graduate of the Marine Corps Command and Staff Course and of the CIA's Mid-Career Course 101.

John D. Stempel is Senior Professor of International Relations at the University of Kentucky's Patterson School of Diplomacy and International Commerce, where he was Associate Director (1988–93) and Director (1993–2003). He came to the University of Kentucky following a 24-year career in the U.S. Foreign Service. There he focused on political and economic affairs, with overseas assignments in Africa (Guinea, Burundi, Zambia), Iran, and India, concluding with three years as U.S. Consul General in Madras. His Middle East service (1975–79) in Tehran provided the material for his book *Inside the Iranian Revolution*. His subsequent academic writings have focused on religion and diplomacy, intelligence and diplomacy, and American views of negotiation. His Washington assignments featured duty for both the State and Defense Departments, including a two-year tour as Director of the State Department's Crisis Center. He has taught at George Washington and American Universities, plus two years as Diplomat in Residence at the U.S. Naval Academy, Annapolis. Stemple is a member of the New York Council on Foreign Relations and is listed in *Who's Who in the World* and *Who's Who in America*. He holds an A.B. degree from Princeton University and M.A. and Ph.D. degrees from the University of California at Berkeley.

Stan A. Taylor is an Emeritus Professor of Political Science at Brigham Young University in Provo, Utah. He has taught in England, Wales, and New Zealand and in 2006 was a visiting professor at the University of Otago in Dunedin, New Zealand. He is founder of the David M. Kennedy Center for International Studies at Brigham Young University. He writes frequently on intelligence, national security, and U.S. foreign policy.

Athan Theoharis is Professor of History at Marquette University whose research has focused on government secrecy, Cold War politics, and the history of the FBI. He is the author, coauthor, and editor of eighteen books, including *The FBI and American Democracy* (2004), *Chasing Spies* (2002), *A Culture of Secrecy* (1998), and *The FBI: A Comprehensive Reference Guide* (1998). He has received numerous awards, including the American Bar Association's Gavel Award and selection as a fellow by the Wisconsin Academy of Arts, Sciences, and Letters.

Gregory F. Treverton is senior analyst at the RAND Corporation. Earlier, he directed RAND's Intelligence Policy Center and its International Security and Defense Policy Center, and he is Associate Dean of the Pardee RAND Graduate School. His recent work has examined at terrorism, intelligence, and law

enforcement, with a special interest in new forms of public-private partnership. He has served in government for the first Senate Select Committee on Intelligence, handling Europe for the National Security Council, and most recently as vice chair of the National Intelligence Council, overseeing the writing of America's National Intelligence Estimates. He holds an A.B. *summa cum laude* from Princeton University, a master's in public policy, and Ph.D. in economics and politics from Harvard University. His latest books are *Reshaping National Intelligence for an Age of Information* (Cambridge University Press, 2001), and *New Challenges, New Tools for Defense Decisionmaking* (edited, RAND, 2003).

Michael A. Turner is a political scientist who has taught international relations and national security matters in San Diego, California, for the past twelve years. Before that, he spent over fifteen years in various positions within the CIA. Turner is the author of *Why Secret Intelligence Fails* (2005; 2006) and the *Historical Dictionary of United States Intelligence* (2006).

Michael Warner serves as Historian for the Office of the Director of National Intelligence.

Nigel West is a military historian specializing in security and intelligence topics. He is the European editor of the *World Intelligence Review* and is on the faculty at the Center for Counterintelligence and Security Studies in Washington, DC. He is the author of more than two dozen works of nonfiction and recently edited *Guy Liddell Diaries*.

Reg Whitaker is Distinguished Research Professor Emeritus, York University, and Adjunct Professor of Political Science, University of Victoria, Canada. He has written extensively on Canadian and international security and intelligence issues.

James J. Wirtz is Professor in the Department of National Security Affairs at the Naval Postgraduate School, Monterey, California. He is Section Chair of the Intelligence Studies Section of the International Studies Association and President of the International Security and Arms Control Section of the American Political Science Association. Wirtz is the series editor for *Initiatives in Strategic Studies: Issues and Policies*, published by Palgrave Macmillan.

Amy B. Zegart is Associate Professor of Public Policy at the University of California, Los Angeles. A specialist on national and homeland security, she has served on the National Security Council staff, as a foreign policy advisor to the Bush-Cheney 2000 presidential campaign, and as a consultant to California state and local homeland security agencies. She has published articles in leading academic journals, including *International Security* and *Political Science Quarterly*, and is the author of *Flawed by Design: The Origins of the CIA, JCS, and NSC* (Stanford, 1999). She received her Ph.D. in political science from Stanford, where she studied under Condoleezza Rice, and an A.B. in East Asian Studies from Harvard University.

STRATEGIC INTELLIGENCE

STRATEGIC INTELLIGENCE

4

COUNTERINTELLIGENCE AND COUNTERTERRORISM: DEFENDING THE NATION AGAINST HOSTILE FORCES

Edited by
Loch K. Johnson

Intelligence and the Quest for Security

PRAEGER SECURITY INTERNATIONAL
Westport, Connecticut • London

Library of Congress Cataloging-in-Publication Data

Strategic intelligence / edited by Loch K. Johnson.
p. cm.—(Intelligence and the quest for security, ISSN 1932-3492)
Includes bibliographical references and index.
ISBN 0-275-98942-9 (set : alk. paper)—ISBN 0-275-98943-7 (vol. 1 : alk. paper)—
ISBN 0-275-98944-5 (vol. 2 : alk. paper)—ISBN 0-275-98945-3 (vol. 3 : alk. paper)—
ISBN 0-275-98946-1 (vol. 4 : alk. paper)—ISBN 0-275-98947-X (vol. 5 : alk. paper)
1. Military intelligence. 2. Intelligence service—Government policy. I. Johnson, Loch K., 1942–

UB250.S6385 2007
327.12—dc22 2006031165

British Library Cataloguing in Publication Data is available.

Library of Congress Catalog Card Number: 2006031165
ISBN: 0-275-98942-9 (set)
0-275-98943-7 (vol. 1)
0-275-98944-5 (vol. 2)
0-275-98945-3 (vol. 3)
0-275-98946-1 (vol. 4)
0-275-98947-X (vol. 5)
ISSN: 1932-3492

First published in 2007

Praeger Security International, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the Untied States of America

The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE

THIS FIVE-VOLUME SERIES IN INTELLIGENCE IS SOMETHING of a landmark in the study of intelligence. Thirty years ago, one would have been hard-pressed to find enough good articles on the subject to fill two volumes, let alone five. In those three decades since 1975, however, the study of intelligence has grown considerably. Today there are several solid professional journals in the field, including the premier publications *Intelligence and National Security* (published in the United Kingdom), *International Journal of Intelligence and Counterintelligence* (the United States), and *Studies in Intelligence* (from the Central Intelligence Agency, in both classified and unclassified form). In just the past two years, bulging anthologies on the general topic "strategic intelligence," as well as a "handbook" on intelligence and a collection of chapters within the more specialized niche of "intelligence and ethics" have appeared, along with a tidal wave of books and articles on one aspect or another of this subject (see the bibliographic essay in volume 1).

Except in times of scandal (Watergate in 1973, CIA domestic spying in 1974, the Iran-*contra* affair in 1987), one could find in this earlier era little newspaper coverage of intelligence activities, so tightly held were these operations by the government. Now, fueled by the events of the September 11, 2001, terrorist attacks and the erroneous prediction in 2002 that weapons of mass destruction (WMDs) were being developed and stockpiled by Iraq, hardly a week goes by without reports on intelligence in the *New York Times* and other leading newspapers. These days, the *Atlantic Monthly* and the *New Yorker*, America's top literary magazines, visit the subject with some regularity, too. The latter has hired Seymour M. Hersh, the nation's most well-known investigative reporter with an intelligence beat.

Intelligence studies has come of age.

Certainly the chapters in these volumes display a breadth of inquiry that suggests an admirable vibrancy in this relatively new field of study. Presented here are empirical inquiries, historical treatments, theoretical frameworks, memoirs, case studies, interviews, legal analyses, comparative essays, and ethical assessments. The authors come from the ranks of academe (twenty-five); the intelligence agencies (thirteen); think tanks (seven); Congress, the State Department, and the National Security Council (three); and the legal world (three).[1] Over a quarter of the contributors are from other nations, including Canada, England, Germany, Israel, Scotland, Switzerland, and Wales. The American writers come from every region of the United States. As a collective, the authors represent a wide range of scholarly disciplines, including computer science, history, international affairs, law, sociology, political science, public administration, public policy studies, and strategic studies. Many of the contributors are from the ranks of the top intelligence scholars in the world; a few young ones stand at the gateway to their academic careers.

Notable, too, is the number of women who have entered this field of study. Thirty years ago, it would have been rare to find one or two women writing on this subject. Seven have contributed chapters to these pages, and another two wrote documents that appear in the appendixes. This is still fewer than one would like, especially in light of the major contribution women have made as intelligence officers. One thinks of the heroic efforts of British women in code breaking and in the Special Operations Executive during World War II, and the American women who contributed so much to the analytic efforts of the Office of Strategic Studies (OSS) during that same war. At least, though, the number attracted to the scholar study of intelligence appears to be rapidly expanding.

The end result of this mix is a landscape illuminated by a variety of methods and appreciations—a rich research trove that examines all the key aspects of intelligence. In addition, each of the volumes contains backup materials in the appendixes. These documents provide the reader with access to significant primary and secondary sources referred to in the chapters.

The volumes are organized according to the major topics of studies in the field. The first volume, titled *Understanding the Hidden Side of Government*, introduces the reader to methods commonly used in the study of intelligence. It imparts, as well, a sense of the "state of the discipline," beginning with a bibliographic essay (by the editor) and continuing with an examination of specific approaches scholars have adopted in their inquiries into this especially difficult discipline, where doors are often shut against outsiders.

In the bibliographic essay that opens the volume, I argue that the literature on intelligence has mushroomed over the past thirty years. Some of this literature is unreliable, but much of it is of high quality. Amy B. Zegart follows my chapter with an important caveat: the literature may be more voluminous these days, but intelligence studies as an academic field has yet to be accepted as a vital part of national security scholarship. The mainstream journals of history, international

affairs, and political science have still regarded the study of intelligence as a marginal pursuit. In this regard, Zegart points out, there is a major disconnect between academic scholarship and those who make decisions in Washington, London, and other capitals around the world.

Following this introduction, Len Scott and Timothy Gibbs look at methods that have been used to study intelligence in the United Kingdom; Stuart Farson and Reg Whitaker in Canada; and Michael Warner in the United States. The volume then turns to a more specific inquiry into the central question of how intelligence is interpreted by professionals—the issue of analysis—explored by John Hollister Hedley. An overview of the sometimes turbulent relationship between intelligence officers and the policy makers they serve is explored by James J. Wirtz; and British scholar Peter Gill recalls the failures associated with the 9/11 attacks and the poor judgments about Iraqi WMDs, in hopes of extracting lessons from these intelligence disasters. In the next chapter, the youngest scholar represented in this collection, Harold M. Greenberg, takes us back in time with a remembrance of the legendary CIA officer and Yale history professor Sherman Kent, often known as the dean of CIA analysts. Kristin Lord rounds out the first volume with a look forward into future prospects for a more transparent world—the ultimate goal of intelligence.

As with each of the books, Volume 1 has a set of appendixes designed to supplement the original chapters with supportive materials from government documents and other sources. Appendix A contains the relevant intelligence excerpts from the National Security Act of 1947—the founding charter for the modern American intelligence establishment. Appendix B provides a history of U.S. intelligence since 1947, prepared for the Aspin-Brown Commission in 1995–96 by staff member Phyllis Provost McNeil. These two documents present a contextual backdrop for the Volume 1 chapters. Appendix C provides "wiring diagrams" of the intelligence community, that is, organizational blueprints for the sixteen agencies and related entities. One chart displays the community as it is today, and another displays how it looked in 1985. As the contrast between the two illustrates, the events of September 11, 2001, have led to a larger and more complex intelligence apparatus in the United States. Appendix D shows a photograph of the CIA Headquarters Building, as an example of what one of the secret agencies actually looks like from an aerial perspective. The white dome in the foreground is an assembly hall seating around 600 people and to its left is the main entrance to the original CIA headquarters, built during the Eisenhower years. Behind this older wing is the new green-glass structure erected during the Reagan administration, often known as the Casey addition because William J. Casey was the Director of Central Intelligence (DCI) at the time of its construction during the 1980s.

Appendix E lists the top leadership in the America's intelligence community: the DCIs from 1947–2005 and today's DNI. Included here as well are the leaders in Congress who have been responsible for intelligence accountability in the past, along with the current members of the two congressional Intelligence

Committees: the Senate Select Committee on Intelligence (SSCI, or "sissy" in the unflattering and sometimes true homophone of Capitol Hill vernacular) and the House Permanent Select Committee on Intelligence (HPSCI or "hipsee"). Appendix F presents a 1955 statement from historian and CIA analyst Sherman Kent about the need for a more robust intelligence literature. He would probably be amazed by how much is being written on this subject now. Appendix G offers an overview on the purpose and challenges of intelligence, drawn from the introductory chapters of the Aspin-Brown Commission Report. Finally, Appendix H provides an opening glimpse into the subject of counterintelligence, a world of counterspies and betrayal taken up more fully in Volume 4.

With the second volume, titled *The Intelligence Cycle: The Flow of Secret Information From Overseas to the Highest Councils of Government*, the focus shifts from a broad overview of intelligence to a more detailed examination of its core mission: the collection, analysis, and dissemination of information from around the world. The National Security Act of 1947, which created America's modern intelligence establishment, made it clear that the collection, analysis, and dissemination of information would be the primary duty of the intelligence agencies. As Allen Dulles—the most famous DCI (America's top intelligence official, until this title changed to director of National Intelligence or DNI in 2005)—put it, the intelligence agencies were expected "to weigh facts, and to draw conclusions from those facts, without having either the facts or the conclusions warped by the inevitable and even proper prejudices of the men whose duty it is to determine policy."[2] The collection and interpretation of information, through espionage and from the public record, would be the primary responsibility of America's secret agencies.

At the heart of this mission lies the so-called intelligence cycle. Professional intelligence officers define the cycle as "the process by which information is acquired, converted into intelligence, and made available to policymakers."[3] The cycle has five phases: planning and direction, collection, processing, production and analysis, and dissemination (see Appendix A in Volume 2 for a depiction). As former CIA officer Arthur S. Hulnick notes, however, in the opening chapter, the idea of a "cycle" fails to capture the complexity of how intelligence is collected, assessed, and distributed by intelligence officers.

The next five chapters in Volume 2 take us into the world of the "ints," that is, the specialized "intelligences" (methods) used by intelligence officers to collect information. Patrick Radden Keefe and Matthew M. Aid probe the method of signals intelligence or SIGINT, a generic term used to describe the interception and analysis of communications intelligence and other electronic emissions, from wiretapping telephones to studying the particles emitted by missiles in test flights. Both authors are sensitive to the possible abuse of these techniques, which can be and have been used to spy on Americans without a proper judicial warrant. Jeffrey T. Richelson explores the IMINT domain, that is, imagery intelligence or, in simple terms, photographs taken by surveillance satellites and reconnaissance airplanes (piloted and unpiloted). Telephone conversations can be revealing, but

in the old saying, a picture can be worth a thousand words. (Appendix B provides photographic examples of these spy platforms, and Appendix C offers illustrations of the IMINT data they can collect.)

Important, too, is information that can be acquired by human agents ("assets") guided by case officers inside the CIA or the Defense Department, the topic of human intelligence or HUMINT, examined by Frederick P. Hitz. Not all the information needed by policy makers is acquired through SIGINT, IMINT, or HUMINT; indeed, the overwhelming majority—upward of 95 percent—is already in the public domain. This open-source intelligence (OSINT) must be sorted through, organized, and integrated with the secretly gained information. Robert David Steele's chapter looks at OSINT and its ties to the other ints.

In the next chapter, Daniel S. Gressang IV dissects some of the technological challenges faced by intelligence agencies in sorting through the avalanche of data that pours into their headquarters from various intelligence collectors around the world. Here is the Herculean task of sorting out the wheat from the chaff (or the signal from the noise, in another widely used metaphor) in the search for information that may warn the nation of impending peril. Here is the vital task of providing "indicators and warnings" (I&W) to a nation's leaders.

One of the most difficult relationships in the complex process of collection, analysis, and dissemination of information comes at the intersection between intelligence professionals and policy makers—groups of individuals that often have very different training, aspirations, and cultures. Jack Davis sheds light on this often turbulent relationship in the United States, and Michael Herman tackles the same topic in the United Kingdom. Minh A. Luong offers a case study on economic intelligence that underscores some of the difficulties encountered as information travels from the collectors and analysts (the "producers" of intelligence) to the policy makers (the "consumers"). Finally, Max M. Holland takes a look at how intelligence agencies examine their own mistakes ("postmortems") and attempt to make corrections—and how political consideration enter into the process.

By way of supporting documentation, in addition to the appendixes already mentioned, Appendix D outlines the general types of reports prepared by the producers of intelligence, along with a listing of specific examples. Appendixes E and F provide samples of key intelligence products: National Intelligence Estimates (NIEs)—the most important long-range and in-depth forecasting carried out by the U.S. secret agencies ("research intelligence," in contrast to shorter intelligence reports that tend to focus on near-term events, or "current intelligence"); Special National Intelligence Estimates (SNIEs), which concentrate on a narrow, high-priority information requirement (say, the capabilities of the Chinese military); and the *President's Daily Brief* (PDB), the most exclusive current intelligence report prepared by the intelligence agencies for the consumption of the president and a few other high-ranking officials.

In light of the fact that every study of the 9/11 and Iraqi WMD intelligence failures find fault, in part, with America's capacity for human intelligence—

especially in the Middle East and Southwest Asia—Appendix G presents one of the most searing critiques of this int. The critique, by the House Permanent Select Committee on Intelligence, has become all the more significant because the panel's chairman, Representative Porter Goss (R-FL), soon after the completion of the report rose to the position of the DCI. Last, Appendix H provides an excerpt from a key report on the Iraqi WMD mistakes, prepared by the "Roberts Committee": the Senate Select Committee on Intelligence, led by Pat Roberts (R-KS).

The third volume, titled *Covert Action: Behind the Veils of Secret Foreign Policy*, enters an especially controversial compartment of intelligence: the means by which the United States attempts to not just gather and analyze information about the world—hard enough—but to manipulate global events through secret activities in the advancement of America's best interests. An ambiguous passage of the National Security Act of 1947 charged the National Security Council (NSC), the boss over the sixteen U.S. secret agencies, to "perform such other functions and duties related to intelligence [over and beyond collection-and-analysis] affecting the national security as the National Security Council may from time to time direct."[4] The phrase "other functions and duties" left the door open for launching the CIA (and more recently the Pentagon) on a wide range of covert actions around the world.

Covert action (CA), sometimes referred to as the "quiet option," is based on the supposition that this secret approach to foreign affairs is likely to be less noisy and obtrusive than sending in the Marines. Sometimes professional practitioners also refer to covert action as the "third option," between diplomacy and open warfare. As former Secretary of State and National Security Adviser Henry Kissinger once put it: "We need an intelligence community that, in certain complicated situations, can defend the American national interest in the gray areas where military operations are not suitable and diplomacy cannot operation."[5] Still others prefer the euphemism "special activities" to describe covert action. Whatever the variation in terminology, the goal of covert action remains constant: to influence events overseas secretly and in support of American foreign policy.

Covert action operations are often grouped according to four broad categories: propaganda, political, economic, and paramilitary (PM) activities. An example of a propaganda operation was the CIA's use of Radio Free Europe during the Cold War to transmit anti-communist themes into nations behind the Iron Curtain. A political CA during the Cold War was the CIA's clandestine funneling of funds to the anti-communist Christian Democratic Party in Italy. An economic example: the CIA attempted to destroy electric power stations in Nicaragua during the 1980s, as a means of undermining the Marxist-oriented S*andinista* regime. PM operations can including everything from assassination plots against foreign heads of state to arming and guiding pro-American insurgent armies in one country or another. Little wonder this has been a controversial subject.

Gregory F. Treverton introduces the reader to covert action in the first chapter of Volume 3. He is followed by Kevin A. O'Brien and Ephraim Kahana, who discuss the use of covert action by other nations. The next four chapters illuminate certain aspects of CA, with James M. Scott and Jerel A. Rosati providing an overview of CA tradecraft (that is, the tools used to implement such operations); Michael A. Turner evaluating the merits of CIA covert propaganda operations; William J. Daugherty looking at political and economic examples of covert action; Jennifer D. Kibbe exploring the entry of the Defense Department into this domain; and former diplomat John D. Stempel contrasting the uses of covert action to diplomatic initiatives. Winding up the volume is Judge James E. Baker's legal analysis of covert action.

Supporting documents include excerpts from the Church Committee Report on the evolution of covert action as carried out by the CIA (Appendix A). The supervision of covert action went from an informal to a highly formal process, as a result of a law known as the Hughes-Ryan Act, passed on December 31, 1974. The language of this statute is presented in Appendix B, and the covert action procedures that resulted from the law are outlined in Appendix C. At the center of the covert action decision process since the Hughes-Ryan Act is the *finding*, a term of art that stems from the passage in the law that requires the president to "find" that a particular covert action proposal is important and has the president's approval. Appendix D contains two findings from the Iran-*contra* era in the mid-1980s. Covert actions must have an organizational apparatus to carry them out, and Appendix E displays what that apparatus looked like during the Cold War (and in basic form remains the organizational chart today, with a few name changes in the boxes).

One of the most controversial forms of covert action has been the assassination of foreign leaders. Appendix F presents a case study from the Church Committee on the CIA assassination plot hatched against the leader of the Republic of Congo, Patrice Lumumba, in 1960. The Committee's exposé of this and other plots led President Gerald R. Ford to sign an executive order prohibiting assassination as an instrument of American foreign policy (see Appendix G). The executive order has been waived in times of authorized warfare against other nations, however, leading to failed attempts to assassinate Saddam Hussein in the first and second Persian Gulf Wars (he was eventually captured alive in 2004, hidden away in a hole near his hometown in Iraq) and Al Qaeda leader Osama bin Laden during the Clinton administration. Considerable ambiguity exists regarding the current status of the executive order and under what conditions it might be waived by administrations. Finally, Appendix H—drawing on a presidential commission study and congressional hearings—examines covert action at its lowest state: the Iran-*contra* affair of the 1980s, when this approach to foreign policy subverted the U.S. Constitution and several laws (including the Hughes-Ryan Act).

A third intelligence mission, after collection-and-analysis and covert action, is counterintelligence (CI) and its associated activity, counterterrorism (CT).

Here is the concentration in Volume 4, titled *Counterintelligence and Counterterrorism: Defending the Nation Against Hostile Forces*. Like covert action, CI went without specific mention in the National Security Act of 1947. By the early 1950s, however, it had similarly achieved a status of considerable importance as an intelligence mission. CI specialists soon waged nothing less than a secret war against antagonistic intelligence services (especially the Soviet KGB); and, after the Cold War, CT specialists would focus on efforts to block terrorists who targeted the United States and its allies. Explaining why the mission of counterintelligence/counterterrorism evolved, a CI expert has pointed out that "in the absence of an effective U.S. counterintelligence program, [adversaries of democracy] function in what is largely a benign environment."[6]

The practice of counterintelligence consists of two matching halves: security and counterespionage. Security is the passive or defensive side of CI, involving such devices as background investigations, fences, sentries, alarms, badges, watchdogs, and polygraphs (lie detection machines). Counterespionage (CE) is the offensive or aggressive side of CI. The most effective CE operation is the infiltration of an American agent or "mole" into the enemy camp, whether a hostile intelligence service or a terrorist cell—a ploy called a penetration. Thus, the practice of security is, according to one of America's top counterintelligence experts, "All that concerns perimeter defense, badges, knowing everything you have to know about your own people," whereas the CE side "involves knowing all about intelligence services—hostile intelligence services: their people, their installations, their methods, and their operations."[7]

Stan A. Taylor and Nigel West clarify these issues in the first two chapters of this volume, then in the next two chapters Katherine A. S. Sibley and Athan Theoharis examine the challenges of keeping the United States spy-free. Rhodri Jeffreys-Jones looks at the efforts in Europe to create a counterintelligence capability similar to that practiced by America's Federal Bureau of Investigation (FBI). Glenn Hastedt takes the reader into the counterterrorism thicket in Washington, DC, explaining how politics influences CI and CT operations. Richard L. Russell and Jennifer Sims discuss the ups and downs of trying to establish an effective counterterrorism response in the United States, complicated by the fragmentation of authority and widely differing cultures among the sixteen U.S. intelligence agencies. Finally, Katharina von Knop looks at the rising role of women in terrorist organizations.

The back-of-the-book documents in Volume 4 begin with a look at the Church Committee findings regarding counterintelligence in 1975 (Appendix A), followed by the notorious Huston Plan—a master counterintelligence spy plan drafted by White House aide Tom Charles Huston in 1970, in response to a nation at unrest over the war in Vietnam (Appendix B). The Huston Plan is a classic illustration of overreaction in a time of domestic strife. In Appendix C, the Senate Select Committee on Intelligence summarizes its findings about the Aldrich H. Ames counterintelligence disaster. Next the appendixes include a series of U.S. commission conclusions about how to improve intelligence in the struggle

against global terrorism, whether locating and penetrating their cells in advance of a terrorist attack or thwarting the ability of terrorists to acquire WMDs. The panel reports include: the Hart-Rudman Commission of 2001 (Appendix D); the 9/11 or Kean Commission of 2004 (Appendix E); and the Silberman-Robb Commission of 2005 (Appendix F). For purposes of comparison, the final appendix (G) examines the conclusions reached by a British commission that also probed the Iraqi WMD failure: the Butler Report of 2004.

The fifth volume in the series, titled *Intelligence and Accountability: Safeguards Against the Abuse of Secret Power*, stems from a concern that secret power might be misused by those in high office. This danger was underscored in 1975 when Congress found the U.S. intelligence agencies guilty of spying against law-abiding American citizens, and again in 1987 during the Iran-*contra* affair when some elements of the intelligence community violated the public trust by ignoring intelligence laws. The United States has been one of the few nations in the world to conduct an ongoing experiment in bringing democratic accountability to secret government activities. Democracy and spying don't mix well. Secrecy runs counter to democratic openness, while at the same time openness possesses a threat to the success of espionage operations. Democracies need intelligence agencies to acquire information that may protect them, but thoughtful citizens worry about having secret agencies in an open society.

Until 1975, the nation's remedy for the tension between intelligence gathering and democracy was to trust the intelligence agencies and hope for the best. Elected officials treated the secret services as exceptional organizations, immune from the checks and balances envisioned by the framers of the Constitution. Lawmakers were satisfied with this arrangement, because if an operation went awry they could duck responsibility. When James R. Schlesinger, DCI in 1973, attempted to inform John Stennis (D-MS), a key member of the Senate Armed Services Committee, about an approaching operation, the Senator stopped him short: "No, no, my boy, don't tell me. Just go ahead and do it, but I don't want to know."[8]

This attitude on Capitol Hill—overlook rather than oversight—underwent a dramatic turnabout in December 1974, however, when the *New York Times* reported on allegations of CIA spying at home and questionable covert actions in Chile. Congress might have waved aside the revelations about Chile as just another Cold War necessity in the struggle against regimes leaning toward Moscow, but spying on American citizens—voters—was another matter altogether. In January 1975, President Ford created the Commission on CIA Activities Within the United States (the Rockefeller Commission, led by his vice president, Nelson Rockefeller). Later that month the Senate established a select committee to investigate intelligence activities. The committee was headed by Frank Church, D-ID, and became known as the Church Committee (the editor served as Church's assistant). A counterpart House committee, led by Representative Otis Pike (D-NY), began investigations the following month.

These various panels, especially the Church Committee, found many more improprieties than they had expected. Not only had the CIA engaged in domestic

spying in violation of its charter, so had the FBI and several military intelligence units. Furthermore, the FBI had carried out secret operations, known collectively as COINTELPRO, against thousands of civil rights activists, members of the Ku Klux Klan, and Vietnam War dissenters. The objective was to make their lives miserable by disrupting their marriages and employment. The Bureau even attempted to blackmail Dr. Martin Luther King Jr. into committing suicide. Church Committee investigators also discovered CIA assassination plots against foreign leaders and efforts to topple President Salvador Allende of Chile, even though he had been democratically elected.

These revelations convinced lawmakers that the time had come to bring accountability into the dark recesses of government. Congress established intelligence oversight committees in both chambers—the Senate in 1976 and the House a year later—and, by 1980, required by law timely reports on all secret intelligence operations. The new Committees pored over intelligence budgets, held regular hearings (mostly in closed session to protect spy sources and methods) and seriously examined the performance of America's intelligence agencies. No other nation has ever so thoroughly applied democratic principles to its secret services, although a number are now beginning to follow the leadership of the United States toward greater intelligence supervision.[9]

Since 1975, this effort has evolved in fits and starts. Sometimes lawmakers have insisted on close accountability, as when they enacted the Intelligence Oversight Act of 1980 with its stringent reporting requirements for covert operations, or when a series of laws in the 1980s sought to end covert actions in Nicaragua. At other times, members of Congress have loosened the reins—for example, repealing in 1985 a prohibition against covert action in Angola. On still other occasions, Congress has concentrated on helping the intelligence agencies improve their security and performance, as with a law in 1982 that prohibited exposing the names of undercover officers. The Iran-*contra* scandal of 1987 was a major setback to this new oversight, as the Reagan administration bypassed most of these rules and statutes in its conduct of a covert war in Nicaragua against the will of Congress. The scandal was an alert to lawmakers. The Intelligence Oversight Act of 1991 further tightened intelligence supervision by clarifying reporting requirements. Lawmakers also set up an Office of Inspector General in the CIA, confirmed by and accountable to Congress.

The pulling and tugging has continued, most recently over whether President George W. Bush violated the Foreign Intelligence Surveillance Act (FISA) of 1978 by conducting warrantless wiretaps as part of the war against terrorism in the aftermath of the 9/11 attacks. The FISA required warrants, but the White House claimed (when the secret operation leaked to the media) the law had become to cumbersome and, besides, the president had inherit authority to conduct the war against terrorism as he saw fit. This debate aside for the moment (several authors address the issue in these volumes), one thing is certain: the intelligence agencies in the United States are now very much a part of the nation's system of checks and balances. Americans want and deserve both civil liberties and a secure defense

against threats; so the search continues for an appropriate balance between liberty and security, democracy and effectiveness—precisely the topic of Volume 5.

The set of chapters on intelligence accountability are introduced with a chapter by David M. Barrett, the foremost authority on the history of accountability in the early years of modern U.S. intelligence (1947 to 1963). The chief counsel of the Church Committee, Frederick A. O. Schwarz Jr., then reflects back on the effects of that watershed inquiry. Next, the editor offers a previously unpublished interview with DCI William E. Colby, who stood at the helm of the intelligence community as it weathered the storm of the investigations into domestic spying during 1975. Mark Phythian presents a chapter on the British experience with intelligence accountability; and, comparing British and American oversight, Lawrence J. Lamanna contrasts the responses on both sides of the Atlantic to the faulty Iraqi WMD assessments in 2002.

The next chapter, written by Cynthia M. Nolan, looks at contemporary issues of intelligence oversight in the United States. Hans Born and Ian Leigh follow with a comparative dimension by contrasting intelligence accountability practices in a variety other nations. Finally, A. Denis Clift and Harry Howe Ransom, who have witnessed the unfolding of intelligence accountability over the past four decades, offer their appraisals of where the experiment stands today.

The first supporting document in this volume is a succinct legislative history of intelligence accountability from 1947 to 1993, prepared by the Senate Select Committee on Intelligence (Appendix A). Then come a series of important oversight laws, beginning with FISA in 1978. With this law, members of Congress sought to rein in the open-ended authority of the executive branch to wiretap and otherwise spy on individuals considered risks to the national security—a privilege abused by a number of administrations from the 1930s forward. Henceforth, FISA required a warrant from a special court (the FISA Court, whose members are appointed by the Chief Justice of the Supreme Court) before such intrusive measures could be carried out. This law, a hot topic in 2005–6 when critics charged the second Bush administration with violation of the warrant requirement, can be found in Appendix B.

The Intelligence Oversight Act of 1980 is presented in Appendix C. This is a brief but nonetheless far-reaching law, enacted by Congress as an attempt to become an equal partner with the executive branch when it came to intelligence. The 1991 Intelligence Oversight Act (Appendix D) emerged after the Iran-*contra* scandal and provided a tightening and clarification of the language in its 1980 precursor, especially with respect to the approval and reporting rules for covert action. The political tug-of-war over the drafting of this currently prevailing oversight statute was intense, leading to the first and only presidential veto of an intelligence act. President George H. W. Bush found the proposal's insistence on prior reporting of covert action objectionable in times of emergency. Lawmakers entered into a compromise with the chief executive, settling on a two-day reporting delay in emergencies. The bill passed Congress again, this time without a presidential veto.

In 1995, the House Permanent Select Committee on Intelligence launched an inquiry into a wide assortment of intelligence issues, stimulated initially by counterintelligence concerns (Aldrich Ames's treasonous activities at the CIA had recently been discovered) but turning into an opportunity for a broad review of new challenges that faced the secret agencies now that the Cold War had ended. In Appendix E, an excerpt from the Committee's final report examines the state of intelligence accountability in the mid-1990s. The next document, in Appendix F, carries the examination into the twenty-first century, with the appraisal of the 9/11 Commission on the same subject. The commissioners were unimpressed, referring to intelligence accountability as "dysfunctional."

At the center of any efforts to maintain accountability for the secret agencies lies the question of funding—the mighty power of the pursue, held in the hands of lawmakers. Appendix G draws on the findings of the Aspin-Brown Commission to provide official documentation about how the United States spends money for spying. Finally, in Appendix H, DCI Robert M. Gates (1991–93) offers observations about oversight from the perspective of the intelligence community management team, located at that time on the Seventh Floor of the CIA.

Here, then, is what the reader will find in these five volumes. The editor and the contributors hope the chapters and documents will help educate the public about the importance of intelligence agencies, as well as stimulate scholars around the world to further the blossoming of this vital field of study. I am pleased to acknowledge my gratitude to Praeger's Heather Staines, senior project editor, and Anne Rehill, development editor, each a pleasure to work with and most helpful in their guidance; Julie Maynard at the University of Georgia for her administrative assistance; Lawrence J. Lamanna, my graduate research assistant, for his good counsel and logistical help; Leena S. Johnson for her indispensable encouragement and support; and the contributors to these volumes for their outstanding scholarship and their much appreciated cooperation in keeping the publishing train running on time.

These volumes are enthusiastically dedicated to Harry Howe Ransom, who has done so much in the United States to lead the way toward a serious discipline of intelligence studies.

Loch K. Johnson

NOTES

1. Some of the authors have had multiple careers, so in categorizing them I have counted the place where they have spent most of their professional lives.

2. Quoted by Senator Frank Church (D-ID), in *Congressional Record* (January 27, 1976), p. 1165.

3. *Fact Book on Intelligence* (Washington DC: CIA Office of Public Affairs, April 1983), p. 17.

4. National Security Act of 1947, signed on July 26, 1947 (P.L. 97-222; 50 U.S.C. 403, Sec. 102).

5. Comment, "Evening News," NBC (January 13, 1978).

6. Editor's interview with a FBI counterintelligence specialist, Washington, DC (May 16, 1975).

7. Editor's interview with Raymond Rocca, CIA/CI specialist, Washington, DC (November 23, 1975).

8. Editor's interview with James R. Schlesinger, Washington, DC (June 16, 1994).

9. See Hans Born, Loch K. Johnson, and Ian Leigh, *Who's Watching the Spies? Establishing Intelligence Service Accountability* (Washington, DC: Potomac Books, 2005).

1

DEFINITIONS AND THEORIES OF COUNTERINTELLIGENCE

STAN A. TAYLOR

Counterintelligence is to intelligence as epistemology is to philosophy. Both go back to the fundamental question of how we know things, both challenge what we are inclined to take most for granted and both offer heavy advantage in debate to those who are skeptical of appearances.

—Thomas Powers[1]

INTRODUCTION

THEORIES ARE DEVELOPED AND USED IN SCIENCE to present conceptual frameworks that allow one to understand and explain phenomena. Theories also generate questions that are useful in research. These frameworks normally consist of assumptions (often called hypotheses) and statements, usually described as necessary and sufficient, for both explanation and prediction. However, in social sciences, the explanatory function is somewhat more important than the predictive function of theory because all of the controls necessary for a predictive theory are not available. Theories in the social sciences can be very useful in *explaining* phenomena but only moderately useful as *predictive* tools in what are called post hoc predictions that are much the same as explanations of historical events. This chapter presents a counterintelligence (CI) theory that explains (to some extent) the existence of counterintelligence practices in any state. The theory is drawn from broader intelligence theories of which counterintelligence is a part.

This attempt to theorize about counterintelligence begins with a brief discussion of intelligence theories and then derives counterintelligence theories from them.

DEFINITIONS AND THEORIES OF INTELLIGENCE

Intelligence scholars argue about definitions of intelligence, but the primary difference between these efforts is merely the expansiveness of the definitions. In its most expansive application, *intelligence* refers to:

- The process that begins when national decision makers identify what information is needed to help them make better informed decisions regarding any entity with which they must deal.
- The prioritization, collection, analysis, production, and use of that information.
- The organizations and groups that actually collect, analyze, and produce the information.
- The other activities of various groups who participate in the intelligence cycle.
- The information and insights that flow from this process.

As defined, intelligence differs from the general use of information by human beings in everyday social intercourse in, at a minimum, six ways:

- The fate of ideologies, nations, economies, and people may depend on how effectively the information or intelligence is utilized.
- The information desired is usually (although not always) information that other individuals, groups, and nations do not want revealed.
- The information desired is about individuals, groups, or nations who often (but not always) are hostile or potentially hostile toward the collecting nation.
- The collection of this information is usually, although not always, done clandestinely.
- Individual, group, or national rights may be violated in the collection of this information.
- The broader intelligence process may generate secret special activities meant to influence the foreign or domestic policies of other states without revealing the source of the influence.

The Latin origins of the word *intelligence* are revealing. The prefix *inter* means between or among. Thus, the term *international relations* refers to the relations between or among nations. The remainder of the word *intelligence* comes from the Latin word *leger*—the gathering of fruit or vegetables. Over time, these two terms were combined into one word referring to the knowledge and skills necessary to distinguish between good and bad fruit and vegetables. Gradually, the meaning of *intelligence* came to connote the skills and aptitudes needed to make wise and productive choices about any aspect of one's life. It is

used in this chapter to refer to the knowledge and information necessary to make informed decisions about statecraft.

Although some scholars stress the difference between intelligence as used by psychologists and intelligence as used by national strategists, in reality they come from the same origins. The word *intelligence* in "intelligence quotient" (IQ) really refers to the human ability to process environmental information into usable and productive knowledge. That is not substantially different from the ability to collect and process information about the interstate environment as a necessary prelude to informed statecraft.

National Security and Intelligence

At the outset, it is useful to understand the relationship between security and intelligence. Two early pioneers in the analysis of state power, Harold and Margaret Sprout of Princeton University, argued that there were five functions or variables by which the power of any state could be analyzed or measured.[2]

1. The information-providing function. How well do states define a need for information and then collect, analyze, and utilize that information?
2. The decision-making function. Can a nation coordinate all of its resources into an effective strategy?
3. The means-providing function. How well can states provide the elements of power needed to achieve strategic goals?
4. The means-utilizing functions. How well can a government utilize or effectively organize all of the means it may possess?
5. The resistance-to-demands function. How resilient is a state to the demands and challenges of other states?

Intelligence operations are critical in the first function, but also play a significant role in the fifth. Demands are more easily resisted when the intentions and capabilities of a threatening state are known. In sum, intelligence is a significant part of state power, and power—the ability to influence other states in a predictable way—is a crucial and critical key to national security.

Theories of Intelligence

Humans use theories to explain observed reality. They are necessary for the development of any discipline. However, only a few scholars have attempted to develop theories of intelligence; among them are David Kahn and Loch K. Johnson.[3] Kahn believes his theory meets the requirements of all theories—it is both explanatory and predictive. He begins with the assumption that all biological organisms, from amoebas to nation-states, need to sense their environment sufficiently to protect their existence. This leads him to his notion that intelligence, by its very nature, is for protection or for defense. That is, it is "essential to survival,

but not to dominance."[4] He discusses both the antiquity and ubiquity of intelligence but notes the changing relative importance between physical intelligence (for example, information about physical objects—tanks, troops, etc.), whose importance is in relative decline, and verbal intelligence (for example, captured communications that may reveal enemy plans), which is increasing in importance. Kahn believes intelligence is increasing in importance, but he acknowledges that it will never be perfect. He also believes that the greatest contemporary and future problem intelligence faces is to be accepted by generals and heads of state whose minds are often set before they view intelligence information.

Johnson's approach is less of a general theory and more specific to strategic intelligence—that is, intelligence needed to support foreign policy and national strategy. He modestly calls his effort a "preface" to a theory and addresses the question of how much of a nation's scarce resources should be devoted to intelligence. He argues that such variables as a nation's global involvement, foreign policy goals, perceived threats, number of intelligence targets, and its ability to consume intelligence information will need to be studied more closely to construct an explanatory and predictive theory of intelligence. Johnson's greatest contribution is his insistence that intelligence must be viewed in the overall context of a nation's global strategy and threats.

A third and more general theory of intelligence, one into which both Kahn's and Johnson's theories would fit quite comfortably, can be drawn from cybernetics, a discipline developed in 1947 by mathematician Norbert Weiner and others.[5] The word *cybernetics* comes from a Greek word meaning helmsman or governor—one who steers a ship. A helmsman must use skill, intuition, and constant feedback from the environment to achieve accurate steerage of the vessel.

Cybernetics is a complex science drawn from biology, neural modeling, psychology, mathematics, electrical engineering, as well as other disciplines. It is the science of feedback—the study of how information can maintain or alter any biological, social, mechanical, or artificial system. Cybernetics has contributed to the development of general systems theory, artificial intelligence, and robotics, as well as significant developments in psychology and learning theories.

It is a perfect paradigm or theory for the role of intelligence applied to statecraft. Decision makers are the helmsmen, the governors, who must use skill, intuition, and a constant flow of information or intelligence to optimize efficiency (defined as the most security at the least cost) for the state. Cybernetics is the iterative flow of information that allows thermostats to maintain temperature in a building, computers to manufacture goods, guided missiles to reach their targets, and human beings to function in an often hostile world. It is about goal-oriented behavior at all levels of living systems. It allows these systems to reach defined goals based on information flows. It is a unifying theory that runs through all levels of human interaction. Though not frequently acknowledged, it played a role in the development of constructivism, particularly social constructivism—the notion that social institutions adapt through the constant processing of stimuli (information) from the environment.

Intelligence, defined as process, product, or people, collects and analyzes stimuli from the international environment. This information is used by decision makers as they act as helmsmen in steering the ship of state through the hazardous waters of international politics.

It should be obvious that all theories of intelligence or counterintelligence are overlaid on the traditional realist approach to international affairs. That is, it is the anarchic nature of global affairs that forces states to look out for their own interests, knowing that no others will look out for those interests for them. As long as states are sovereign, and as long as there is no ultimate authority among states, intelligence will be collected by all states, and counterintelligence efforts will be taken to protect state secrets.

COUNTERINTELLIGENCE

Counterintelligence "refers to the efforts taken to protect one's own intelligence operations from penetration and disruption by hostile nations" or groups and to protect state secrets.[6] Its primary functions are to:

- Protect classified information from unauthorized disclosure.
- Collect information about foreign intelligence services to prevent them from obtaining classified information from your nation.
- Collect information about hostile or potentially hostile group or state sponsored intelligence services to prevent them from disrupting or compromising your own operations through penetration, disinformation, or other means.
- Identify and recruit foreign intelligence agents to feed false and misleading information through them; that is, to "double" them and use them for your own purposes.

Counterintelligence Techniques

Several techniques, practices, and procedures are necessary to perform the primary functions.[7]

PRE-EMPLOYMENT PERSONNEL SECURITY

All intelligence community (IC) employees, as well as all people who handle classified information, are subject to background checks. These background checks begin with biographical information but include interviews with people who have known the applicants. For many IC agencies, this background check may also involve a polygraph or lie detector test. Although some scholars doubt the validity of the polygraph, few doubt that the fear of "being put on the box" has a deterring effect. While the Central Intelligence Agency (CIA), the National

Reconnaissance Office (NRO), the Defense Intelligence Agency (DIA), and the National Security Agency (NSA) have used the polygraph for many years, the Federal Bureau of Investigation (FBI) only began to polygraph employees after the disastrous Robert Hanssen case. Hanssen had spied for both the Soviet Union and Russia for about twenty-two years and would most likely have continued had his treason not been revealed by another spy who knew of his activities.

IN-SERVICE PERSONNEL SECURITY

Each agency also monitors its own employees during their period of employment. Many require periodic polygraph tests during which the employees are asked questions about their lifestyles as well as about foreign contacts and classified material they have handled. Other aspects of employee lifestyles—such as dramatic changes in financial worth, changes in spending habits, or aberrant sexual practices—are also observed independently and may provide questions for future polygraph sessions as well as act as warning signs to counterintelligence officers.

FACILITY SECURITY

Successful counterintelligence is impossible if facilities where secrets are produced and stored are not secure. Every agency in the IC as well as government offices, institutes, businesses, and contractors that handle classified information are responsible for facility security. Often this will also include computer security. Facility security varies widely from location to location, and some of America's worst security breaches have occurred at defense contractor facilities. It is the responsibility of IC counterintelligence officers to monitor security at all of these sites and to takes actions when that security is lax.

COMMUNICATIONS SECURITY

Overall communications security in the United States is the responsibility of the NSA, which provides, maintains, and verifies secure communications equipment at most IC agencies and other offices that handle classified information. However, each agency also carries out some communications security functions within its own facilities.

CLASSIFICATION AND COMPARTMENTATION

Information that might reveal sensitive national security secrets is classified by the government. Information may be classified both vertically and horizontally. There are three horizontal levels of classified information—confidential (used with decreasing frequency), secret, and top secret. Top secret information may be divided into vertical divisions called codeword compartments. The

information in each compartment usually comes from a unique and specific intelligence collection source. That is, top secret/codeword material derived from a particular human source will be classified top secret and given a unique codeword. Information derived from intelligence intercepts of encrypted Soviet government communications throughout the 1950s, for example, was classified as top secret/Venona. A person's access to compartmented information is given on a need-to-know basis. That is, is knowledge of the particular information necessary for the performance of the person's official duties?

Issues of classification and compartmentation are continual thorns in the side of democratic governments. Virtually no one believes they protect classified information as they should, but virtually everyone agrees that governments have a legitimate right to keep sensitive national security information secret.

SIGNALS INTELLIGENCE

All intercepted communications are searched for clues that might reveal foreign agents operating in the United States or that might reveal U.S. persons working under foreign control. For example, the Venona project, already mentioned, was begun in 1941 by Army security and taken over by the NSA when it was created in 1952. The names of many well-known American and British traitors—Klaus Fuchs, Kim Philby, Alger Hiss, Julius and Ethel Rosenberg, just to name a few—were revealed through Venona decrypted information.

PROSECUTING TRAITORS

Antiespionage laws are not effective unless penalties exist for revealing or stealing secret information. Foreign agents in the United States who are caught stealing secrets or receiving classified information will be jailed if they do not have official cover, or they will be declared persona non grata and deported if they are in the country as a representative of their governments under official cover. U.S. citizens or U.S. persons who are caught revealing classified information are subject to federal prosecution.

Catching foreign agents or their American assets is a complicated task, primarily under the direction of the FBI. The Bureau, on the one hand, has a long history of detecting law breakers, gathering solid evidence against them, and then relying on the Department of Justice for prosecution. The CIA, on the other hand, prefers to detect traitors, monitor their activities, and use them as leads to other traitors and spies of whom they might not be aware. Rather than prosecuting them, they might wish to double them or supply them with misleading information. The clash between these two cultures has created a strained relationship between these two agencies marked by an absence of collaboration and cooperation of legendary proportions. And as has often been said, the success of counterintelligence in America rises or falls with the level of cooperation between the FBI and the CIA.

The counterintelligence techniques and practices listed here constitute an arsenal of no small significance. Nevertheless, the record of counterintelligence within the United States is not particularly distinguished. As William Webster, former director of both the FBI and the CIA, stated before U.S. Senate hearings in 2002, "Almost every spy that we have found both in the CIA and the FBI, has been found with the aid of recruited sources of our own in other hostile intelligence agencies."[8] In fact, from William Sebold, the German American recruited by German intelligence in 1939 who voluntarily became a double agent for the FBI, down to the most recent Americans caught in the act of treason, the information revealing them generally has come from defectors or from security files obtained from foreign states.

The testimony of former senior Soviet military spymaster Stanislav Lunev before the U.S. House of Representatives does not add any luster to the record of American counterintelligence. According to Lunev, "Despite the tireless work of the men and women of [US intelligence agencies], I must honestly report to you that obtaining highly sensitive and classified information was not very difficult."[9] In his testimony, Lunev went on to describe that while posing as a Soviet journalist, he attended the official unveiling of the Stealth aircraft, took photographs of highly sensitive parts of the aircraft, and sent them to Soviet military analysts to see what they could learn from them.

Assumptions of Counterintelligence Theory

Counterintelligence arises from the existence of four conditions or assumptions. First, it assumes that a nation has a decision-making system that deals with information that in the hands of hostile groups or nations, could jeopardize national security. Second, it assumes that a nation has one or more intelligence services that collect that information and then try to prevent it from falling into enemy hands. Third, it assumes that foreign intelligence services will attempt to obtain other nations' classified information through normal intelligence procedures (human intelligence and signals intelligence) as well as attempting to identify some who possess classified information and enticing them to reveal it. Fourth, a theory of counterintelligence assumes a very low level of trustworthiness in virtually all people. This last assumption will be discussed at greater length shortly.

These assumptions add up to a theory of counterintelligence that explains the existence of CI activities in the intelligence services in all internationally active nations. The first three assumptions fit nicely into each of the theories of intelligence discussed earlier. Counterintelligence is primarily defensive—it attempts to protect national secrets from other groups or nations in whose hands that information might be harmful. Kahn's theory of intelligence stresses its defensive value, a subsidiary function of which is counterintelligence. Johnson's theory is also useful in understanding counterintelligence. Among other things, it suggests that the extensiveness of a nation's global involvements explains the extensiveness and the costs of intelligence services. And the scope and

extensiveness of a nation's intelligence services also explains both the efforts and the funds necessary to protect the security of the information collected.

The cybernetic theory of intelligence is what is called a "grand theory"—it explains a large variety of human behavior from which more narrow and specific activities can also be explained. As applied to the field of intelligence and counterintelligence, this theory also works very well. Nations require information so that decision makers can steer the ship of state safely through the hazardous waters of international politics. That information or intelligence diminishes in value if it is known to other nations or groups, particularly hostile ones. In fact, counterintelligence is essential for intelligence to be useful. Revealed classified information is more dangerous than the absence of information because it means that the steering of the ship of state may be based on false information, on information describing conditions that no longer exist, or on information deliberately revealed to deceive. Uncertainty about a state's environment may be better than unwarranted certainty, and the illusion of security may be worse than the absence of any intelligence services at all. As Thomas Powers has written,

> An insecure [intelligence] service is not merely useless; it is positively dangerous, because it allows a hostile agency to manipulate the penetrated organization, as the British, for example, manipulated German intelligence during World War II. MI 5 turned German agents in Britain, used them to feed false information to Germany, and thereby thoroughly confused the Germans as to the probable site and nature of the invasion of Europe. The Germans would have done better with no agents in Britain at all. . . . It is better to have no intelligence service at all than to have one which is insecure.[10]

Trust

More must be said about the fourth assumption of counterintelligence—the absence of trust—because it is particularly critical to an understanding of counterintelligence. Were all people fully trustworthy, many CI functions would be unnecessary. Most elements of personnel security and certain aspects of facility security (checking briefcases and packages that leave secure facilities, for example) would be unnecessary, and there would be few or no traitors to prosecute. Communication lines would still need to be made secure, and captured communications of other states would still have to be mined to see if foreign agents had penetrated any agencies or facilities, but it is the absence of trust that makes much of counterintelligence necessary.

This assumption is a human-level application of realism. It is based on that notion that for whatever reasons, humans possess an inherent dark side that causes them to doubt the goodness of others. Human nature is flawed, as Niebuhr and other realists have argued. Thus, they must always take steps to see that they are not hurt by their trust of others. When sixteen-year veteran CIA officer Harold Nicholson attempted to justify selling classified information to the Soviet Union, he explained that because his work had kept him away from his family and

prevented him from being a good father, he thought he needed to look out for his own interests for once and earn some extra money for his family.

Not only is distrust the basis of much counterintelligence, but its very practice magnifies its presence. It is a curious conundrum—an automatic and self-feeding cycle that ultimately degenerates into paranoia and worse. The act of counterintelligence quite literally feeds feelings of suspicion, which in turn create greater distrust. And a culture of distrust spawns disgruntled employees who are ripe for recruitment by foreign intelligence services. In his 1953 play *Camino Real*, Tennessee Williams has the following dialogue:

John: "Why does disappointment make people unkind to each other?"

Marguerite: "Each of us is very much alone."

John: "Only if we distrust each other."

Marguerite: "We have to distrust each other. It is our only defense against betrayal."

As two former CIA employees have written, "The function of the counter-espionage officers is to question and verify every aspect of CIA operations; taking nothing at face value, they tend to see deceit everywhere. In an agency full of extremely mistrustful people, they are the professional paranoids."[11] Counterintelligence officers must distrust their fellow employees, look suspiciously at the good faith of—and even challenge—defectors, and study foreign intelligence entities so thoroughly so they begin to think like foreign intelligence agencies and officers.

James Jesus Angleton, the legendary and controversial director of CIA counterintelligence for over twenty years, described the landscape of counterintelligence as "a wilderness of mirrors," an "ever-fluid landscape where fact and illusion merge."[12] It is not an easy environment in which to work. Rebecca West has noted that "people who work in a self-contained [counterintelligence] unit are apt to develop theories which develop none the better for never being subject to open discussion."[13]

It is widely believed that Angleton's culture of distrust pervaded the CIA for so long that counterintelligence gained a very bad reputation within the agency—a reputation that lingered long after Angleton's forced resignation in 1974. In reaction to this culture of distrust, employees tended to question the need for both counterintelligence functions and officers. They tended to believe that their fellow officers who had been vetted and cleared and were in the service of their country could be trusted. It was a notion somewhat like joining a community service or business club; once a Rotarian, for example, one could be trusted forever.

This anticounterintelligence culture may have contributed to the failure to detect subsequent traitors throughout the entire IC. For example, the treason of Aldrich Ames, a CIA officer who spied for the Soviet Union and then for Russia for nine years, was nurtured partially by this culture. Information he sold resulted in the betrayal and death of nearly all of the CIA's most productive Soviet assets

at the height of the Cold War. Time and time again, a failure to take counterintelligence seriously, in part a reaction against the Angleton years, resulted in ignoring clear signals of Ames's treason.

On his just under $70,000 a year salary, Ames paid cash for a $540,000 home, purchased a $40,000 red Jaguar automobile (which he drove to work), and had money left over for cosmetic dental surgery. Ames once even cited Angleton's legacy as a reason for his decision to spy.[14] Whether this statement is true or merely his attempt to blame someone else for his actions, it is undoubtedly true that counterintelligence was not taken as seriously as it should have been at that time.

Sources of Treason

This trust-distrust paradox was first stated by first-century Roman philosopher and statesman Seneca in his *Letters to Lucilius*: "It is a vice to trust all, and equally a vice to trust none." But whom can you trust? This dilemma has provoked many to study the causes of betrayal and treason. It turns out that although many traitors on both sides of the Iron Curtain, particularly during the early years of the Cold War, were motivated by ideology, money has been the primary motivation of treason since the mid-1970s.[15] But if one examines secondary motives, that is, motives that led to ideological betrayal or selling out for monetary gain, the role of disgruntlement is growing. If one "considers those who, though not completely disgruntled, were not entirely 'gruntled' (to borrow from Oscar Wilde), then disgruntlement becomes a more prevalent motive" for treason.[16]

If the "trust assumption" aspect of counterintelligence theory is correct, then it may well be that a substantial part of the defense against treason in the future may be played by the human resources personnel in each intelligence agency. The ability to keep personnel satisfied with their employment may be one of the better defenses against treason, particularly against treason for financial gain. How to accomplish that is not the purpose of this chapter, however; enlightened and responsive leadership and management, collegial work conditions, the absence of cronyism in salary and advancement decisions, fair rewards for quality service, work equality, and employees who have bought into the mission of the agency for whom they work are certainly beginning points. Perhaps Andrew Roberts captured a glimpse of what was coming when he wrote in 1997, "Tomorrow's traitors are more likely to be driven to betray not from ideological convictions but from whining complaints about poor pension provisions or underfunded performance-related pay."[17]

SUMMARY AND CONCLUSION

This chapter began by defining intelligence, discussing how intelligence relates to national security, and then offered a brief review of three compatible and interrelated theories of intelligence. This was followed by a definition of

counterintelligence, a summary of the primary functions of counterintelligence, and a review of CI techniques. Following that, four assumptions about counterintelligence were presented. These four assumptions provide a basis for a counterintelligence theory. At a general level of activity, this theory explains the existence of the practice of counterintelligence in virtually all states. The level of both intelligence and counterintelligence activities, as Johnson argues, depends on the extensiveness of a state's global activities and obligations.[18]

The absence of trust within societies appears to be the primary assumption in the theory of counterintelligence. Were all people trustworthy, much counterintelligence work would be unnecessary. That being the case, those who guard government secrets need to devote more time and energy into developing and nurturing trustworthiness within their employees. At the same time, a related effort needs to be made to reduce the rather high levels of disgruntlement among the custodians of national secrets.

This is a difficult task when, of necessity, the functions of counterintelligence are dispersed and decentralized throughout the IC and when the very practice of counterintelligence tends to alienate some employees. Clearly, the counterintelligence staff in every agency needs to take their work more seriously. Both routine as well as random security investigations need to be standard procedure rather than something done only when a traitor has been revealed. Perhaps the advice of the Countess to Bertram in Act I, Scene I, of Shakespeare's *All's Well That Ends Well* ought to be followed: "Love all, trust a few, do harm to none."

Counterintelligence personnel need to be well trained. There is a tendency to assume that any intelligence professional can be moved in and out of counterintelligence without additional training. And counterintelligence needs to be done in the field as well as at the home office. CI officers need to be rewarded within their field of specialization. Many feel that they need to get out of CI and into better career tracks or even to leave their agency and work in private industry. Counterintelligence is taken seriously in the United States only after a traitor has been revealed. After FBI agent Robert Hanssen was caught, the FBI acknowledged that it did not take security seriously. After CIA officer Aldrich Ames was caught, CIA officials acknowledged the same.

Finally, counterintelligence is the most difficult of all intelligence work. It is a thankless task where practitioners are in a lose-lose situation. If spies are found within U.S. agencies, it is called a counterintelligence failure. If they are not found, it may also be called a counterintelligence failure. What is often called the Law of Invisible Phenomena must be kept in mind: The absence of evidence is not evidence of absence.

NOTES

I thank the following for their help at various stages of the writing of this chapter: Kara Norman, Eric Lindsay, and Victoria Taylor.

1. Thomas Powers, *The Man Who Kept the Secrets: Richard Helms and the CIA* (New York: Knopf, 1979), cited in Charles E. Lathrop, *The Literary Spy* (New Haven: Yale University Press, 2004), 54.

2. Harold and Margaret Sprout, *Foundations of National Power: Readings on World Politics and American Security*, 2nd ed. (New York: Van Nostrand, 1962), 167–75.

3. David Kahn's theory is found in "An Historical Theory of Intelligence," *Intelligence and National Security* 16 (2001): 79–92; Loch K. Johnson's theory is found in "Preface to a Theory of Strategic Intelligence," *International Journal of Intelligence and Counterintelligence* 16 (2003–2004): 638–63.

4. Kahn, "An Historical Theory of Intelligence," 80.

5. This section is drawn from Stan Taylor, "Security and Intelligence," chapter 14 in Alan Collins, ed., *Contemporary Security Studies* (Oxford: Oxford University Press, 2006).

6. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 2nd ed. (Washington, DC: CQ Press), 113.

7. The best available list of all counterintelligence techniques is found in Frederick L. Wettering, "Counterintelligence: The Broken Triad," *Intelligence and National Security* 13 (2000): 265–300.

8. Cited in Lathrop, *The Literary Spy*, 58.

9. Lunev's testimony was before the House National Security Committee on August 8, 1998, and is cited in Lathrop, *The Literary Spy*, 55.

10. Powers, *The Man Who Kept the Secrets*, as cited in Lathrop, *The Literary Spy*, 49.

11. Victor Marchetti and John Marks, *CIA and the Cult of Intelligence* (New York: Knopf, 1974), cited in Lathrop, *The Literary Spy*, 52.

12. The phrase actually comes from T. S. Eliot's 1920 poem "Gerontion." It has also been used as the title of several books, including one by former CIA officer David Martin in 1980 about Angleton. The subsequent quotation comes from Norman Polmar and Thomas B. Allen, *Spy Book: The Encyclopedia of Espionage*, 2nd ed. (New York: Random House Reference, 2004), 685.

13. *The New Meaning of Treason* (New York: Time, 1966), cited in Lathrop, *The Literary Spy*, 51.

14. Pete Early, *Confessions of a Spy* (New York: Putman's Sons, 1997), 146.

15. See Stan A. Taylor and Daniel Snow, "America's Cold War Spies: Why They Spied and How They Got Caught," *Intelligence and National Security* 12 (1997): 101–25. The best work on treason is done by the Defense Personnel Security Research Center in Monterey, California. See, for example, Susan Wood and Martin F. Wiskoff, *Americans Who Spied Against the Country Since World War II* (Monterey, CA, 1994); Lynn F. Fischer, "Espionage: Why Does It Happen," at http://www.hanford.gov/oci/maindocs/ci_r_docs/whyhappens.pdf, accessed (December 20, 2005); as well as Theodore R. Sabin and others, *Citizen Espionage: Studies in Trust and Betrayal* (Westport, CT: Praeger, 1994).

16. Taylor and Snow, "America's Cold War Spies," 110.

17. Andrew Roberts, *Sunday Times* (London), May 25, 1997, as cited in Lathrop, *The Literary Spy*, 398.

18. Johnson, "Preface to a Theory of Strategic Intelligence."

2

VENONA AND COLD WAR COUNTERINTELLIGENCE METHODOLOGY

NIGEL WEST

THE ROLE PLAYED BY VENONA IN COUNTERINTELLIGENCE operations conducted during the Cold War has been well documented since the decrypts were declassified and released to the public in July 1995. We now know, for example, that Alger Hiss was a Soviet spy, both Ethel and Julius Rosenberg were guilty of espionage, and such important figures in the Roosevelt administration as Harry Dexter White at the Treasury Department and Lauchlin Currie in the White House were part of a massive network directed from Moscow. VENONA proved to be the Holy Grail for British and American counterintelligence specialists to the extent that it provided leads to and offered links between hundreds of suspects. It also served to corroborate information from other sources, such as the testimony of Elizabeth Bentley, the NKVD (Narodnyy komissariat vnutennikh del, the Soviet foreign intelligence service) defector who was the catalyst for more than 100 FBI investigations following her statement made to special agents in September 1945.[1]

The attraction of VENONA is that in a sometimes murky counterespionage environment, it is as close to empirical evidence as can be found, but the paradox is that in legal terms the material was completely worthless and was never adduced in any criminal trial. The decrypts were, after all, the subjective application of cryptanalytical processes that could easily be refuted or undermined by defense counsel in any trial. In addition there was concern about maintaining secrecy of the nature of the source. At the time, the code breakers had narrowed the field of potential traitors to Klaus Fuchs and his friend the physicist Rudolf Peierls, who both appeared to fit the profile prepared by the mole hunters, VENONA remained an active source, with the Soviets continuing to rely on a compromised cipher system. Not surprisingly the Anglo-American teams working on the project were anxious not to alert their adversaries to the scale of the security breach, so even after the

source appeared to terminate, with the Soviet introduction of new procedures, there was a keen desire to keep what had been achieved thus far as secret as possible. We now know that the Soviets received at least three warnings that their communications had been jeopardized. First, there is the recollection from Bentley that Currie had conveyed a message from his post in the White House as early as 1944 alerting the NKVD to the fact that the Americans had broken some of their traffic. Then, in 1947, a VENONA text concerning Judith Coplon indicated that the Americans had learned some of the code names routinely used for certain Washington institutions, such as the FBI (HUT) and the State Department (BANK).[2]

How could they have learned this? The most probable source of the leak was William Wiesband, a Russian linguist employed at Arlington Hall as an interpreter who had been indoctrinated into the project in 1945, as had his wife. Because neither were ever charged with espionage, Wiesband's status as one of the most important spies of the twentieth century has gone largely unrecognized outside of the Allied signals intelligence community, where he is still regarded as the discipline's most damaging traitor. The extent to which his wife assisted him, consciously or unconsciously, is unresolved. However, KGB retirees, such as Yuri Modin, have acknowledged that Wiesband tipped them off to the breakthrough accomplished by the Armed Forces Security Agency.[3] And equally certainly, it is acknowledged by all concerned that Kim Philby received a briefing on the project before he left London to take up his liaison role in Washington, DC, in September 1949.[4]

Indeed, Philby boasted in his 1968 memoirs, *My Silent War,* that he had immediately conveyed a message to his Soviet contact about the lapse, although his version suggests Soviet censors had a hand in concealing the precise details, doubtless to avoid embarrassment by admitting the appalling blunder that had allowed their opponents a window of opportunity which had been exploited so successfully. Certainly VENONA played a key role in the identification of Klaus Fuchs, and although he was convicted and imprisoned in 1950, neither he nor his MI5 interrogator, Jim Skardon, knew anything about the cryptographic source that had compromised him. Skardon was never indoctrinated into VENONA and knew only that the physicist had definitely spied for the Soviets while working on the Manhattan Project during World War II. This absence of doubt gave him a significant advantage, as did Fuchs's naiveté (bordering on intellectual arrogance) in his belief that his actions had not been criminal. During several interviews conducted over three months, Skardon persuaded Fuchs to confess that he had passed classified information to his Russian contacts, and the scientist proved so cooperative that he had subsequently identified an FBI surveillance photograph of Harry Gold as his principal Soviet contact in the United States. Nevertheless, it was VENONA that had supplied the first clues to the existence of a spy at Los Alamos in 1944 code-named REST and CHARLES, and it had taken five years of investigation to narrow the suspects down to Fuchs.

The Fuchs case (known to and filed by the FBI as FOOCASE) raises an interesting issue because Philby kept abreast of the investigation as it closed in on

the physicist, and even before his departure for the United States he had sent a warning to the Soviets that the spy code-named CHARLES was in grave danger. He had been unable to deliver this vital message personally because his last meeting with his contact in London, Mikhail Shishkin, code-named ADAM, had taken place on September 21, before his indoctrination, so he had entrusted the information to Guy Burgess who, inexplicably, failed to pass it on for five months. When the news finally reached the London *rezidentura* on February 10, 1950, Fuchs had been under arrest for eight days. This was an astonishing lapse on the part of Burgess, then drifting in and out of an alcoholic haze, but it also served to suggest to the British and American mole hunters that the integrity of their source was intact, whereas in fact Moscow had made the necessary changes to their ciphers in 1949, unaware than Fuchs was already in dire peril. This all too human blunder on Burgess's part had the severest consequences, for as a result of Fuchs's arrest and confession, Harry Gold was identified, and thereafter the domino effect led to the electric chair for the Rosenbergs.

If, alternatively, Philby's warning had been relayed properly by Burgess, and Fuchs had been withdrawn before he could be interrogated, their subsequent history would have been very different indeed, with Gold and the Rosenbergs probably escaping, too. Understandably, this episode caused consternation in Moscow.

According to Philby's message to Burgess, the Americans had worked on the Soviet traffic for years, with minimal success, but the British Government Communications Headquarters (GCHQ) had achieved impressive results recently. Burgess later insisted that he had included Philby's tip in a personal note that had been photographed by Anthony Blunt, together with other documents, and then handed to Yuri Modin. Naturally, Moscow was alarmed by this news, particularly when Shishkin confirmed that Philby had said nothing about the decryption effort when they had met on September 21. Certainly Modin had received three rolls of film from Blunt on October 11, but when the pictures had been developed they had been found to be overexposed and out of focus. As for Burgess's personal note, it was re-examined in Moscow and found to say nothing about CHARLES.[5]

At their subsequent meeting, held on October 25, 1950, Burgess had promised to recopy the documents, and on December 7 had produced 168 documents, totaling 660 pages, but no personal note. Thus a combination of Blunt's camera error and Burgess's forgetfulness had ensured that the warning about Fuchs failed to reach Moscow. Burgess had said nothing to Modin, and Philby had been out of contact with his handlers while he had settled into his new post in America. Fuchs, of curse, could have been exfiltrated in September or even December 1949, and at the very least he could have been briefed on how to resist an MI5 interrogation, although the *rezidentura* had been out of direct touch with the spy since mid-1949. Although Fuchs seemed quite oblivious to the gravity of his situation and his imminent peril, there was actually no solid evidence against him, so his confession was vital to MI5. A simple, persistent denial would have stymied his adversaries.

According to Modin, reporting on their meeting on February 10, 1950, Burgess reacted with "calm and composure" to the news of the physicist's arrest but accepted that a mistake had been made. Soviet intelligence immediately suspended contact with Burgess and Blunt for six weeks, but Burgess failed to turn up at the next scheduled rendezvous on March 20, 1950, nor did he show up at any of the prearranged back-up meetings. However, at the beginning of April he left emergency signals for Modin and contact was restored on April 17. "Instead of YAN, PAUL came to the meeting without materials," reported the *rezidentura* (referring to Blunt and Burgess, respectively), which submitted a lengthy report on the crisis to Moscow by courier rather than cipher.[6]

Apparently Burgess had not attended the meetings in March because Philby (code-named STANLEY) had been summoned to London by the British Secret Intelligence Service (SIS) to discuss the Fuchs affair. Philby's account of the VENONA project, as he understood it, is illuminating:

> STANLEY asked to communicate that the Americans and the British had constructed a deciphering machine which in one day does "the work of a thousand people in a thousand years," Work on deciphering is facilitated by three factors: (1) A one-time pad was used twice; (2) Our cipher resembles the cipher of our trade organisation in the USA; (3) A half-burnt codebook has been found in Finland and passed to the British and used to decrypt our communications. They will succeed within six to twelve months. The CHARLES case has shown the counter-intelligence service the importance of knowing the past of civil servants. Although STANLEY is trusted, [Valentine] Vivian considers that STANLEY's past is not entirely clear. A role in establishing STANLEY's past may be played by his first wife who is somehow connected to the CHARLES case. STANLEY, PAUL and YAN consider that the situation is serious. A long meeting is needed to discuss it.[7]

The meeting was arranged for May 15, and Modin was instructed to calm Burgess and arrange a further meeting for him with the *rezident*, Nikolai Korovin, for June 4. Modin's meeting with Burgess was "businesslike" and he was "very calm, self-possessed, unhurried."

When Burgess offered to give Korovin at the next meeting a bundle of Foreign Office documents about the recent conference of the three foreign ministers, Modin forbade him. The second meeting with Korovin was held in a quiet suburban park and lasted six and a half hours. The marathon length was accounted for by the anxieties of the Cambridge spy-ring about the threat posed to them by the new menace, described as the "decryption machine," which was the latest generation of GCHQ's computers, then completely unknown to the wider public, that had only recently become aware of relatively primitive automated data processors and card sorters. Korovin admitted that mistakes had been made in the Soviet cipher procedures but tried to reassure Burgess that the errors had been limited and only occurred in wartime. He insisted that no "supermachine" existed capable of cracking the Soviet codes.

Korovin's reassurance is curious and raises the question of whether he was attempting to blithely calm the Cambridge Five or convey an informed message from Moscow. In fact, of course, the mole hunters were by then on the trail of both CHARLES and another quarry, code-named HOMER, who was revealed in April 1951 as Donald Maclean.

The most immediate worry in 1950 was Philby's safety. Burgess relayed to Korovin that Blunt had explained how, during the period in 1940 when the network had been out of direct contact with the *rezidentura*, their communications had been maintained through Edith Tudor-Hart, who had passed information to Bob Stewart of the Communist Party of Great Britain (CPGB). Blunt had recalled that during his conversations with Litzi Philby, she had mentioned the desirability of recruiting an atomic scientist, and he had gained the impression that she had found a suitable candidate. He was worried that if her nominee had been Klaus Fuchs, he might compromise her. It followed that if Fuchs exposed Litzi, the entire network would be put in jeopardy, but Korovin had assured Burgess that Fuchs was unconnected with Litzi. He subsequently submitted a report on the meeting for the *rezidentura*, which reached Moscow.

Before Burgess bade Korovin farewell, he returned to his preoccupation about exposure:

> Before leaving for the United States STANLEY asked PAUL to communicate to us his personal request for granting him political asylum in the USSR in case of obvious danger. PAUL added that essentially it was also a question of granting asylum to him, PAUL. YAN, like STANLEY and PAUL, was strongly alarmed by recent events but showed no signs of cowardice and made no hasty conclusions. In PAUL's opinion, if serious danger threatens, YAN will commit suicide. PAUL said that YAN's moral qualities are not like STANLEY's and PAUL's. STANLEY and PAUL think themselves politicians who have gone through the hard school of life, know what struggle is and know they should achieve their aim. PAUL considers YAN a good comrade, entirely devoted to our cause, but the spirit of an intellectual which is characteristic of YAN's profession is still firm in him, and this spirit makes him accept the inevitable and he doesn't mobilise for the struggle.[8]

Dismayed by Blunt's gloomy prognosis, Korovin asked Burgess to point out the senselessness of Blunt's frame of mind and persuade him to "abandon all thoughts of suicide." Burgess, Philby, and Blunt "can certainly count on our help," insisted Korovin, but when he announced that further personal meetings would have to be suspended, Burgess replied that he "saw no signs of danger" and that he was ready to resume passing documents, either originals, on film, or in the form of personal notes. Korovin declined the offer and provided a new procedure for establishing contact. He concluded the meeting on an optimistic chord: "PAUL was in a good mood. He came to the meeting sober. He thanked me for a long time for my conversation with him and asked to assure the Centre [Soviet intelligence] that everything was all right with him and that he would wait for instructions about passing over material to us."[9]

This meeting was something of a milestone, and it was not until July 1, 1950, that Ivan Chichayev (code-named ROSS) and Mikhail Shishkin had prepared "a summary of ROSS's talk with PAUL." Its conclusion, endorsed by the London rezidentura, was:

> Taking into account the absence of any dangerous signs concerning THE FIVE to conduct the prearranged meeting with PAUL in the first half of July at which to arrange for a meeting with YAN in a month's time for receiving materials. In future to receive documents from PAUL and YAN only on undeveloped film and at personal meetings. To give consent to the *rezidentura*'s suggestion about continuing work with PAUL and YAN and to receiving materials from them.[10]

On July 1, it was Burgess, not Blunt, that went to the arranged meeting and, in accordance with instructions, he arrived empty-handed. He gave an oral account of the war in Korea and said that he would be departing to the United States on July 28. At his next meeting, held on July 8, he passed over a film of Foreign Office papers and received instructions on how to establish contact with the Soviets in Washington, D.C.

Thus, as the mole hunters had disposed of Fuchs and were closing in on Maclean, the Soviets seemed oblivious to the escalating dangers posed by the VENONA project and more concerned about the security of personal meetings with rezidentura personnel. Fuchs had pleaded guilty to charges of breaches of the Official Secrets Act, so his trial had taken only a matter of hours for sentence to be pronounced, and no mention had been made of how MI5 identified him as a spy in the first place. In any event, the Soviets could not have harbored any illusions about how Fuchs had been caught, and their apparent complacency in letting the net narrow around Maclean is chilling. Philby had given what would prove to be a very accurate forecast of the progress that would be achieved by the cryptanalysts, yet his controllers seemed willing to allow both him and Burgess to remove themselves from London, where they might have been in a position to influence events or protect Maclean. It may be that the Soviets felt unable to intervene when their two best spies announced their new postings, and Philby's transfer from SIS's Istanbul station to Washington must have seemed to them like hitting the intelligence jackpot. Nevertheless, the ineptitude with which Soviet intelligence handled the deteriorating situation does seem breathtaking, especially when one considers that Philby hardly knew Maclean and had to guess for himself the true identify of the mole code-named HOMER.

From Philby's perspective, Burgess's arrival in Washington must have been quite a relief and at the very least a welcome opportunity to discuss the growing crisis with him privately. Burgess, of course, was the Cambridge Five's puppetmaster and knew the full ramifications better than anyone else. Alone, the two men would have been bound to consider their options, talk about the likelihood of Blunt's suicide, and debate tactics to save Maclean.

The Fuchs example demonstrated how easily a network could unravel and the skill of the FBI, which had zeroed in on Harry Gold and enabled the scientist

to identify him from a photograph when he had never learned his true name. Fuchs probably had not realized the likely consequences of this identification, and it is obvious he tried to protect his original contact, Ursula Kuczynski, whose true name was also unknown to him. She was, however, already familiar to MI5 as an espionage suspect because she had been denounced by Allan Foote in 1947 and had been interviewed by Jim Skardon on that occasion. The encounter had proved unproductive—she had denied any involvement in Soviet espionage in England, and at the time MI5 had no choice but to accept her denials. Nevertheless, she had fled the country as soon as Fuchs's arrest had been announced.[11]

If Maclean had cracked under questioning in the same way, what might he have disclosed? He knew nothing incriminating about Kim Philby or the other member of the Cambridge Five, John Cairncross, but apart from Burgess and Blunt he could have exposed Kitty Harris, his former lover and NKVD handler in prewar London and Paris. By 1951 Harris was safely back in the Soviet Union, having completed her last assignment as an illegal in the United states, so Maclean really only represented a threat to Burgess and Blunt, and of course his own wife, Melinda, in whom he had confided shortly before their marriage in France in 1940.[12]

While the mole hunters had been searching for CHARLES, other VENONA texts, eight in all, implicated Judith Coplon, who had appeared in the traffic with the code name SIMA. These intercepts made the FBI realize in 1948, as the first text of January 1945 had indicated, that a spy had been at work in the Justice Department in Washington. As soon as Special Agent Bob Lamphere extracted the vital date of the spy's commencement in her new post, February 15, 1945, on an internal transfer from New York, Coplon's identity was confirmed by Inspector Leo Lauchlin in consultation with the assistant attorney-general as SIMA, for she was the only person to have switched from the Justice Department's Economic Warfare section to Washington, as had been mentioned in the traffic.[13]

Preliminary inquiries into Coplon's background showed that her parents were living in Brooklyn, and she had graduated in 1943 from Barnard College, where she had been involved briefly with the Young Communist League. The question for the FBI was how she could be caught on a charge of espionage, bearing in mind that her position gave her access to files on the FBI's current investigations, which doubtless was why no prosecutions had resulted from the allegations made by Elizabeth Bentley. By the time the FBI had gone in pursuit of the members of Nathan Silvermaster's network, there was absolutely no incriminating evidence to be found, even in the extensive photographic laboratory discovered in the basement of his suburban home. Quite obviously, Coplon had allowed the NKVD to remain one step ahead of the FBI, tipping off the Soviets each time a new suspect came under the FBI's scrutiny, so the only action to be taken was the removal of suspects from their jobs. This had effectively eliminated the spy-rings headed by Silvermaster and Victor Perlo but had allowed their subordinate members to evade prosecution. As Coplon was routinely handling internal security dossiers at her office in the Foreign Agents Registration section of the Justice Department, her hand in their escape was all too obvious. The only

advantage to the FBI was to learn which personalities currently under investigation were of interest to the Soviets. In this way suspicion hardened against Joseph Bernstein, a courier whose name appeared on one of the FBI files compromised by Coplon.

Coplon was placed under discreet surveillance, which revealed that she was having an illicit affair with Harold Shapiro, a Justice Department attorney, and that she made two trips a month to New York to visit her parents. When she was followed to Manhattan on January 14, 1949, she was seen to meet a man for dinner who subsequently was identified as Valentin A. Gubitchev, an employee of the United Nations secretariat, and they were watched at two further meetings, on February 18 and March 4. At this latter rendezvous, both were arrested, and Gubitchev was found to be carrying an envelope containing $125, and Coplon's handbag revealed a wealth of classified data, including some documents that had been prepared by the FBI as a barium meal to test whether she gave them to her Soviet contacts.

At her trial, the FBI concealed the exact nature of the "confidential informant" that had led the investigation of Coplon, and she deployed the defense that her relationship with Gubitchev was entirely romantic and the information she had been carrying was nothing more than notes she had prepared for writing a novel. The prosecution neatly destroyed the "innocent liaison" ploy by disclosing details of her affair with Shapiro, so she was convicted and received a sentence of between forty months and ten years' imprisonment for conspiring to pass classified secrets to Gubitchev, who was also convicted.

Coplon's conviction was later overturned on appeal on the technicality that the FBI's telephone intercept had been unlawful. Because the clear impression had been left that the FBI had begun its investigation as a consequence of a wiretap on Coplon's office line, all the evidence that flowed from that source was deemed inadmissible. The alternative was to reveal that the FBI had been led to Coplon by VENONA, but that expedient was considered too high a price to pay, so she was freed to marry one of her lawyers, Albert H. Socolov, and settle in Brooklyn, where she opened several restaurants.

As well as losing Coplon, the FBI also missed Flora Wovschin, code-named ZORA, the daughter of Russian immigrants who had been responsible for Coplon's recruitment in the first place. She, too, had joined the Communist Youth League at Barnard College and later went to work for the Office of War Information in Washington. In 1947 she had resigned from the civil service to marry an Amtorg engineer, but by the time the FBI had started to look for her in 1949 she had moved to Moscow. No action was taken against her mother and stepfather, but the FBI did attempt to identify the other members of her network. The fact that Flora had continued to be active after the war was revealed in a VENONA text from Moscow dated March 11, 1945, marking Stepan Apresyan's appointment to be *rezident* in San Francisco, which designated Vladimir Pravdin (code-named SERGEI) as her controller, with a *referentura* clerk, Olga V. Khlopkova (code-named JULIA), responsible for processing her information:

[16 groups unrecoverable] in San Francisco the work of ALBERT's [Iskhak Akhmerov] office. The operational direction of ZORA [6 groups unrecovered] JULIA [Olga Khlopkova] will deal with his documents under SERGEI's [Vladimir Pravdin] direction.

The scale of Wovschin's activities can be judged by this cable, sent from Moscow two days later:

Your 203. ALAN—Ralph Bowen, works in the BANK [State Department] as assistant [3 groups unrecovered] economics. He and his wife Sue are acquaintances of ZORA and together with the latter were members of the GYMNASTIC organisation [Young Communist League]. In so far as ZORA works in the BANK, [5 groups unrecovered] with them the former friendly relations.

DROP—Philip E. MOSELEY. Up to 1943 worked in the Russian Section of the HUT [OSS]. Since 1943 has been in the BANK in the Division of Territorial Studies. In 1932–34 has [2 groups unrecovered] member of the staff of HARVARD University and [42 groups unrecovered] friend of BLERIOT. According to the latter's information is progressively inclined.

DUVER—our PROBATIONER [agent] in VADIM's office.

ROBERT—connected with the NEIGHBOURS.

OSWARD—Benjamin GERIG [6 groups unrecovered] in the BANK. We have no other data on [1 group unrecovered].

Whether Wovschin remained active until her departure for Moscow is uncertain, but her absence ensured the FBI made no further progress in its pursuit of her. According to the CIA, she participated in anti-American propaganda operations during the Korean War and died soon afterward.

The parallel cases against Fuchs and Coplon serve to illustrate the way in which the VENONA source fitted into the investigative jigsaw puzzle, and while offering an unrivaled glimpse into the adversary's activities, most certainly did not guarantee a criminal conviction or even ensure that espionage could be disrupted. In the example of Coplon, the central figure, Wovschin, was never even interviewed by the FBI, and some of the other personalities mentioned as her recruits were never identified.

The two best-known cases of Soviet espionage exposed by VENONA were those of Klaus Fuchs and Donald Maclean, although the latter defected to Moscow in May 1951 before he could be confronted. Other spies, who might have achieved similar notoriety, also escaped justice. Lauchlin Currie, Joel Barr, and Al Sarant moved abroad. Harry Dexter White died of a heart attack in 1948, and Laurence Duggan, formerly Roosevelt's aide, committed suicide. Although plenty of other spies were to emerge in the VENONA material, among them Ted Hall, Kim Philby, Morris and Lona Cohen, and Bill Wiesband, none of these names were broken by the cryptographers in time to ensure the mole hunters could take full advantage of the information. Indeed, Wiesband's identification as LINK was not made until the declassification process was under way, more than

two decades after his death in May 1967. Actually, the only VENONA traffic directly relevant to contemporaneous counterintelligence operations were the cables exchanged between Moscow and Canberra in 1948, which were read within days of their interception.

Close study of VENONA's counterintelligence value reveals that the raw texts were a component in a larger canvas constructed with contributions from defector testimony (mainly from Elizabeth Bentley, Whittaker Chambers, and Hede Massing), physical and technical surveillance conducted by the FBI, and confidential information extracted from informants whose identities are still protected. These bland categories give no clue to the dramas they concealed: the illicit wiretaps routinely carried out by FBI technicians; the black-bag jobs performed by teams of skilled burglars whose illegal activities were authorized at the highest levels of government; the vast photo libraries of espionage suspects that accrued during street investigations; the monitoring of the vehicle registration plates of cars parked in the vicinity of suspected subversive gatherings; the wholesale penetration of the Communist Party of the United States of America (CPUSA) by legions of paid informants. Only the tiny tip of this investigative iceberg ever surfaced, so it is hard to assess the precise proportion any one indicator gave in the identification of a VENONA code name. Some of the identities were obvious, with the cover names proving semi-transparent or the real name being referred to in plain text, whereas others were much more elusive, and some were demonstrably wrong. The best example of error is the famous blunder in which RELAY was named as Morton Sobell, whereas Professor Philip Morrison was the more likely candidate.

Unquestionably VENONA deserves its reputation as the keystone of Anglo-American counterintelligence investigations, and the fact that the project was not closed down until 1979 suggests its long-term utility, but its longevity conceals some stark realities: VENONA did not implicate Philby or Burgess until it was too late to exploit it. Only Klaus Fuchs was imprisoned as a direct consequence of the source, and his conviction could have been avoided if the Soviets had acted on the information that we now know was available to them at the time.

NOTES

1. Elizabeth Bentley's *Out of Bondage* did not include all the names of spies she identified in her November 1945 statement to the FBI, which has now been declassified.

2. Judith Coplon's prosecution is best described by Marcia and Thomas Mitchell in *The Spy Who Seduced America* (New York: Invisible Cities Press, 2002).

3. In his autobiogaphy *My Five Cambridge Friends* (London: Hodder Headline, 1995), Modin incorrectly identified the source of the NKVD's information about VENONA.

4. Kim Philby, *My Silent War* (London: McGibbon & See, 1968).

5. Nigel West and Oleg Tsarev, *Crown Jewels* (New Haven, CT: Yale University Press, 1999).

6. Ibid.

7. Ibid.
8. Ibid.
9. Ibid.
10. Ibid.
11. Ruth Werner, *Sonia's Report* (London: Chatto & Windus, 1991).
12. Kitty Harris, *The Spy with Seventeen Names* (London: St Ermin's Press, 2001).
13. Robert Lamphere, *The FBI-KGB War* (New York: Random House, 1986).

BIBLIOGRAPHY

Adamson, Iain. *The Great Detective*. London: Frederick Muller, 1966.

Albright, Joseph, and Marcia Kunstel. *Bombshell*. New York: Random House, 1997.

Bamford, James. *The Puzzle Palace*. Boston: Houghton, Mifflin, 1982.

Belfrage, Cedric. *Something to Guard*. New York: Columbia University Press, 1978.

Benson, Robert Louis, and Michael Warner. *VENONA: Soviet Espionage and the American Response 1939–1957,* Washington, DC: National Security Agency, 1996).

Bentley, Elizabeth. *Out of Bondage*. New York: Devin-Adair, 1951.

Bly, Herman O. *Communism: The Cold War and the FBI Connection.* New York: Huntingdon House, 1998.

Burt, Leonard. *Commander Burt of Scotland Yard*. London: Heinemann, 1959.

Carpozi, George. *Red Spies in Washington*. New York: Trident Press, 1965.

Clark, Ronald. *J.B.S.* London: Quality Books, 1968.

Clubb, O. Edmund. *The Witness and I*. New York: Columbia University Press, 1974.

Dallin, David. *Soviet Espionage*. New Haven, CT: Yale University Press, 1955.

Foote, Alexander. *Handbook for Spies*. London: Museum Press, 1964.

Haldane, Charlotte. *Truth Will Out.* London: Vanguard Press, 1950.

Harris, Kitty. *The Spy with Seventeen Names*. London: St Ermin's Press, 2001.

Huss, Pierre J., and George Carpozi. *Red Spies in the UN*. New York: Coward-McCann, 1965.

Kahn, David. *The Codebreakers*. London: Wiedenfeld & Nicolson, 1966).

Kalugin, Oleg. *The First Directorate*. New York: St Martin's Press, 1994.

Klehr, Harvey. *The Secret World of American Communism*. New Haven, CT: Yale University Press, 1995.

Klehr, Harvey, and Ronald Radosh. *The Amerasia Spy Case.* Charlotte: University of North Carolina Press, 1996.

Knightley, Philip. *The Hack's Progress*. London: Bloomsbury, 1997.

Kuczynski, Ruth. *Sonia's Report.* London: Chatto & Windus, 1991.

Lamphere, Robert. *The FBI-KGB War*. New York: Random House, 1986.

Mitchell, Marcia and Thomas. *The Spy Who Seduced America.* New York: Invisible Cities Press, 2002.

Modin, Yuri. *My Five Cambridge Friends.* London: Hodder Headline, 1995.

Montagu, Ivor. *The Youngest Son*. London: Lawrence & Wishart, 1970.

Moorhead, Alan. *The Traitors*. London: Harper & Row, 1952.

Moynihan, Daniel Patrick. *Secrecy*. New Haven, CT: Yale University Press, 1998.

Peake, Hayden. *OSS and the VENONA Decrypts, 12 Intelligence & National Security* (July 1997), pp. 14–34.

Peierls, Rudolf. *Bird of Passage*. Princeton, NJ: Princeton University Press, 1985.
Philby, Kim. *My Silent War*. London: McGibbon & Kee, 1968.
Radosh, Ronald, and Joyce Milton. *The Rosenberg File*. New York: Holt, Rinehart & Winston, 1983.
Rees, David. *Harry Dexter White*. New York: Coward, McCann & Geoghegan, 1973.
Report of the Royal Commission, Canada, 1946.
Report of the Royal Commission, Australia, 1956.
Smyth, Henry D. *Atomic Energy for Military Purposes*. Princeton, NJ: Princeton University Press, 1945.
Stone, I. F. *The War Years, 1939–45*. Boston: Little, Brown, 1988.
Werner, Ruth. *Sonia's Report.* London: Chatto & Windus, 1991.
West, Nigel, and Oleg Tsarev. *Crown Jewels*. New Haven, CT: Yale University Press, 1999.
Wright, Peter. *Spycatcher.* New York: Viking Penguin, 1987.

3

CATCHING SPIES IN THE UNITED STATES

KATHERINE A. S. SIBLEY

FROM THE MOMENT OF THE AMERICAN REVOLUTION, when plotters like Benedict Arnold and John André attempted to snuff out the nascent republic, through the aftermath of September 11, 2001, when terrorists' attacks on the World Trade Center and the Pentagon stunned Americans and created a crisis that is still unfolding, national anxiety over the domestic influence of foreign spies and conspirators has seldom disappeared from American political culture. Catching them has remained a high priority.

John André was perhaps the first spy to be executed by Americans. Sneaking through American lines holding a passport for "John Anderson," with Arnold's plans for the British to take West Point hidden in his stockings, André was intercepted by Continental troops, who turned him in rather than accept proffered bribes of his steed or his watch. André was sentenced to death and hanged on October 2, 1780. Yet despite some celebrated espionage cases in the next major American conflict, the Civil War—including that of Confederate spy Rose O'Neal Greenhow, a well-connected Southerner who infiltrated Northern elite circles, continued spying from prison, and was eventually deported back to the Confederacy—more than a century passed after André's execution before the U.S. government set up intelligence agencies to look for spies. During the 1880s, in response to a growing imperialist push abroad as well as the increased value placed on "professional expertise" at home, the Navy and the War Department both set up intelligence offices, the Navy's in 1882, and the War Department's in 1885. By 1889, the War Department's new Division of Military Information was sending military attachés to five countries. Still, its intelligence-gathering role was rather passive until the Spanish-American War, when Division staff assisted in furnishing information about Cuba and uncovering insurgent plots in

the Philippines. Afterward, this work once again was neglected as the Division suffered from a bureaucratic squeeze that banished it to a remote corner of the capital. Even so, the Justice Department went ahead and set up its Bureau of Investigation in 1909, which played a pivotal role in catching spies later.

For the military, another war was necessary for any revitalization of intelligence collection, and thus it was not until May 1917 that the indomitable Maj. Ralph Van Deman was able to overcome the resistance of top brass to create a newly powerful Military Information Section, despite his superiors being perfectly content with what intelligence the British and French deigned to share with the War Department. It was high time; espionage was already key to the U.S. war effort, thanks to the (British) discovery of the Zimmerman Telegram three months earlier, and its exposure of a German-Mexican plot against the United States. Van Deman also set up a Code and Cipher Bureau during the war to decode foreign cable traffic, which was led by Herbert Yardley and known as the Black Chamber.

The military's intelligence operation thus grew rapidly and included both positive and negative divisions: "positive," to gather information about other countries, and "negative," to stop them from picking up intelligence here. It was in the negative, or counterintelligence function that van Deman particularly excelled, setting up machinery to oversee both the armed forces and civilian populations, whom he deemed as riddled with subversive foreigners. Foreign agents were indeed active; as early as 1914, German military attaché Franz von Papen had organized a sabotage, espionage, and subversive campaign against the United States, which was discovered in 1915 when his agent, Dr. Heinrich Albert, foolishly left his briefcase—full of plans and money—on a train. Albert, von Papen, and other German and Austrian conspirators were soon thrown out of the country, but this did not prevent their successors from engineering the massive Black Tom explosion of 1916, blowing up millions of tons of munitions in northern New Jersey that were headed for Britain.

As the Army's efforts to find spies thus accelerated during the war, so did those of Congress. In 1917, it passed the Espionage Act, which included a $10,000 fine and twenty years' imprisonment for such acts as preventing the recruitment of armed forces personnel, refusing to enlist, or revealing information related to defense. The act sent nearly 1,000 Americans to prison in World War I, including Eugene Debs and Emma Goldman. (Debs was sentenced to ten years in 1918 for speaking out against the act and was pardoned by President Warren G. Harding in 1921; Goldman was sent to prison for opposing the draft, and was then deported to Russia in 1919.)

Van Deman's Military Information Section also officially encouraged private groups such as the American Protective League, also founded in 1917, to identify dissenters. Its thousands of members raided leftist groups like the International Workers of the World but unearthed few spies. Following the war, the Justice Department's Bureau of Investigation went on a massive raid of its own, otherwise known as the Red Scare, arresting more than 1,500 and sending nearly 250 back to Russia on the *Buford*.

A postwar cooling-off period followed the wartime hysteria, although this more relaxed atmosphere also permitted many spies to operate unheeded in the United States during the 1920s and 1930s. Ex-spy Whittaker Chambers believed that the 1930s were, in fact, the heyday of Soviet espionage: "To this period belongs the recruiting of the best Soviet sources. . . . The secret service rode along for almost a decade simply exploiting, and seldom seeking to amplify, this corps."[1] Chambers himself is best known for his filching of State Department documents supplied by Alger Hiss in the mid- to late 1930s, though he had contacts at numerous government departments. He even worked in military espionage, meeting a mathematician at the Aberdeen Proving Ground who supplied him classified materials on aircraft bombsights. Dwight D. Eisenhower later admonished his interwar predecessors for their largely nonexistent counterintelligence response to such practices and blamed it on domestic culture: "The American public has always viewed with repugnance everything that smacks of the spy."[2]

Yardley's outfit did continue for a time as part of the State Department; its most important achievement was spying on Japanese representatives at the Washington Naval Conference and thus learning their negotiating points. But much of the other intelligence work established by van Deman fell by the wayside, and the Black Chamber itself was abolished in 1929, owing in part to Secretary of State Henry Stimson's view that "Gentlemen do not read each other's mail." The Army was less scrupulous; in 1930, it set up the Signals Intelligence Service (SIS) to intercept signal traffic, break codes, and train cryptologists. It was this agency that began to collect secret Soviet communications in World War II, in a project code-named VENONA, which led to the later discoveries of atomic spies detailed below.

In 1930 Congress also conducted an investigation into communist activities, under the leadership of Hamilton Fish (R-NY). Upset by its findings, the Fish committee recommended that alien communists should be deported and Party members should be prevented from using the mails. In line with public opinion in this period, however, newspapers responded critically, arguing that Fish and company exhibited "symptoms of the sort of mental stampede that should be reined in by . . . long established American ideals."[3]

Despite the severe limitations on investigative activity in this era, spies were occasionally foiled. In 1931, William Disch, who designed firing control instruments for the Navy, met a man called Herb, posing as a German spy, who wanted to pay up to $2,000 for the technology. The Office of Naval Intelligence allowed Disch to supply Herb with obsolete blueprints. Bureau of Investigation agents soon spotted Herb taking the documents not into the German embassy but into Amtorg, the Soviet trading agency in New York. Even so, agents had no idea then about the far greater amounts of secret information being provided to Amtorg by Philadelphia chemist Harry Gold, who repeatedly raided the technology of his employer, Pennsylvania Sugar, preparing himself for a far more ambitious atomic espionage career in World War II. In this cautious era, not even J. Edgar Hoover,

director of the newly named Federal Bureau of Investigation (FBI), was ready to have his agenda expanded into investigating "Communistic inner circles," especially if it placed the Bureau in the light of "Agents Provocateur."[4]

As a result, not only Soviet but German agents as well had a field day. In the mid-1930s, Dr. Ignatz Griebl, a German-born Nazi sympathizer living in Manhattan, recruited some of his German patients to spy for the fatherland; they succeeded in garnering blueprints from the Bath Iron Works, the Boston Navy Yard, and the Douglas Aircraft Corporation, among others. Griebl's work was part of a larger ring associated with Guenther Gustave Rumrich, an American educated in Austria. Thanks to a tip from British military intelligence, in 1938 the FBI arrested Rumrich and his associates; however, fourteen of the men charged escaped, including Griebl. This botch was only one of the FBI's missteps in the disastrous persecution of the case, which culminated in the firing of its chief investigator for signing a publicity contract. Despite the errors, the FBI's crime-fighting profile had already been considerably enhanced in this era with its successes in the Lindbergh kidnapping case and several celebrated bank robberies. When Europe's turn to war in August 1939 put the country in a state of emergency, the agency took on a new role in counterespionage work.

Hoover was now no longer shy in packaging his agency as a bulwark against the threatening clouds from abroad. That summer, Franklin D. Roosevelt set up an Interdepartmental Intelligence Committee made up of the FBI, the War Department's Military Intelligence Division, and the Navy's Office of Naval Intelligence and pronounced that "no investigation . . . into matters involving actually or potentially any espionage, counterespionage, or sabotage" could be undertaken except by those three agencies.[5] But Hoover quickly and effectively gained sole jurisdiction over domestic espionage and sabotage outside military personnel. His agency would brook no rivals; armed with its mandate from the White House, the FBI was intent "to head the Nation's attack against foreign spies, saboteurs, and subverters," as Hoover told the American Legion.[6]

The Bureau grew accordingly. Between 1940 and 1945, FBI agents mushroomed from 900 to almost 5,000. And from 1933 to 1945 the Bureau's budget expanded from $2.7 million to $45 million. The ineffectiveness of other agencies (like the State Department) to hinder their own species of spy also expanded the Bureau's purview abroad; in 1940, following the arrest for espionage of Tyler Kent, a disgruntled code clerk at the American embassy in London, FBI undercover agent Louis Beck came snooping and found incredibly lax disposal of secret materials and disturbingly intimate relations between embassy staff and local prostitutes.

Another success for the FBI was its crafty handling of a Nazi ring revealed in 1940 by defector William G. Sebold, an aircraft mechanic who had spied for Germany. Sebold's organization had been gathering military-industrial information in the United States since the 1920s, including the Norden bomb sight and Goddard's rocket technology. With Sebold's able help, the Bureau actually managed the ring, supplying fake but appetizing information that the mechanic

radioed to his counterparts in Germany. When it was finally cashed in by the Bureau, the investigation brought thirty-three convictions and effectively ended German spying in the United States.

During the war, the heightened secrecy surrounding the atomic bomb made discoveries of Soviet espionage even more profoundly disturbing than the feckless attempts of the Germans. Indeed, as Hoover believed, during the war "American Communists . . . made their deepest inroads upon our national life."[7] Scholars have noted the heightened intensity of this wartime anti-Soviet campaign, but it has been judged a "counterintelligence failure" because the United States caught relatively few spies.[8] Yet FBI surveillance forced such Soviet representatives as Harry Gold's wartime handler Semyon Semyonov, NKVD agent Vassili Zarubin, and others to return to Russia, while U.S. officials effectively stymied such military-industrial spies as Clarence Hiskey, Andrei Shevchenko, Arthur Adams, Steve Nelson, and Joseph Weinberg. Soviet intelligence agents could ignore U.S. counterespionage activities only at their peril.

One of the first Soviet spies to be arrested was Gaik Ovakimian, an engineer who worked at Amtorg. Ovakimian was charged with being an unregistered representative of the Soviet government, but he was also known to be a spy; during his stay in the United States, he had paid handsomely for information on the production of gasoline- and on oil-refining processes. Yet after the German invasion of Russia, the State Department dropped the charges against Ovakimian, and he was allowed to return home in exchange for six others. While pursuing Ovakimian, FBI agents also bumped into Soviet master spy Jacob Golos, who had earlier also gotten in trouble as an unregistered foreign agent. The surveillance of Golos did lead the agency to a brief encounter with his lover and spy associate, Elizabeth Bentley, until she lost her pursuers in the Pennsylvania Station ladies' room.[9] Once the United States became firmly committed to helping the Soviet Union, surveillance of the couple ended. They, along with Julius Rosenberg's group of electrical engineers, Harry Gold's industrial and military contacts, Igor Gouzenko's revealed ring of radar and nuclear specialists in Canada, and of course, the large number of sources within the Manhattan Project itself, were largely unhindered participants in a huge haul of material for the Soviet Union in World War II.

Oblivious to all this, the government blundered even more strikingly with Gen. Walter Krivitsky, who actually presented himself as a source on Soviet espionage. Kritivsky, a senior GRU agent who had escaped to the United States in 1938, drew much interest in a series of articles he wrote for the *Saturday Evening Post*. Krivitsky told the State Department's Passport Office of the existence of hundreds of agents, but because there were as yet no procedures for handling defectors, little was done to delve seriously into his allegations. Hoover questioned Krivitsky's ideological leanings, and the Immigration and Naturalization Service was soon trying to deport him. He died in Washington in 1941 under mysterious circumstances. [10]

Krivitsky was not the only defector whose significance was overlooked. Whittaker Chambers had visited Assistant Secretary of State Adolf Berle in

September 1939 to tell him about a network in the State Department and other agencies involved in "Russian espionage." But Berle did not mention Chambers's story to the FBI until March 1940, and it took the Bureau another two years to even contact Chambers. Hoover, of course, could not pursue Soviet espionage to the extent he might have wished. As he told lawmakers, in his counter-espionage program "emphasis was placed upon control of Axis agents operating in the US and upon the penetration and study of the Axis intelligence system."[11] In this, he was effective; German espionage was nearly nonexistent during the war. The handful of inept Abwehr spies who washed ashore on the Eastern Seaboard in 1942 (Long Island, Florida) and 1944 (Maine) were either executed or given long sentences. Another rarity in the United States, a spy for Japan called Velvalee Dickinson, a doll saleswoman who wrote messages about U.S. Navy ships in doll-code, was also captured by the FBI in 1944 after some of her letters were traced. She was sentenced to ten years in prison.

Despite these successes, the far more expansive and effective Soviet espionage operation remained largely unmolested. American officials were hampered in grasping the full dimensions of it by strategic considerations, namely, the alliance with Russia against Nazi Germany. Nevertheless, in 1943 intelligence officials discovered the work of California communist leader Steve Nelson, a Soviet spy interested in developments at the Berkeley Radiation Laboratory, where Ernest O. Lawrence and J. Robert Oppenheimer were conducting early atomic research for the War Department. Nelson's home was already under surveillance when one of Oppenheimer's graduate students came to tell the party leader about his secret work in fall 1942. Then, on March 29, 1943, Nelson was overheard at his home securing "some highly confidential data regarding the nuclear experiments" at the Radiation Lab from another lab scientist, Joseph Woodrow Weinberg.[12] Weinberg provided Nelson a formula that concerned the calutron, a separator that would enrich uranium. Soon after this meeting, Nelson was spotted passing information to Soviet vice consul Peter Petrovich Ivanov. Then, on April 10, the man who headed NKVD activities in the United States, Vassili Zarubin, stopped to visit Nelson and paid him for additional information.

With less justification, intelligence officials were also monitoring J. Robert Oppenheimer during the war. Lt. Col. Boris T. Pash believed that the physicist was passing on material to persons who, in Pash's estimation, "may be furnishing . . . [it] to the Communist Party for transmission to the USSR."[13] As newly unearthed documents reveal, Oppenheimer was almost certainly a party member, but allegations of his involvement in espionage activity have never been convincingly demonstrated.[14] In August 1943, however, Oppenheimer told Army security officers of a breach at the lab. Sometime the previous winter he "had learned from three different employees of the atomic bomb project . . . that they had been solicited to furnish information, ultimately to be delivered to the USSR." None of the men had cooperated, according to Oppenheimer, so he refused to name them; nor, for some months, would he identify the man who had

solicited their espionage, whom he later divulged was Berkeley French professor Haakon Chevalier. That Oppenheimer did not get in more trouble over his reticence may be explained by his having "benefited from exceptional treatment," as one scholar has noted. Despite Oppenheimer's well-known left-wing past, it was only in the 1950s that he found himself subject to the security standards that had destroyed others, and his tale of the three contacts, which he later admitted he had invented, played a crucial role in the loss of his security clearance then.[15]

Occasionally, officials were able to successfully derail Soviet espionage during the war, as they did in their dealings with Soviet Purchasing Commission representative Andrei Shevchenko. On discovering his queries for secret documents, the FBI worked with a librarian and later an engineer at Bell Aircraft to give Shevchenko everything he had asked for on advanced airplanes in sanitized form.[16] The FBI was gratified to learn later that Soviet intelligence considered the doctored material supplied to Shevchenko "reliable." [17] But in December 1945, Shevchenko left the country with his wife and son. His escape had been facilitated not only by a tip from Moscow but also by the U.S. government's apparent reluctance to press charges in the wartime environment. Also departing that month, and for the same reason, was another longtime industrial spy, Arthur Adams.

The FBI had discovered Adams's meetings with Arthur Hiskey, a scientist in the Manhattan Project's University of Chicago laboratory, relatively late in the war. A break-in to Adams's dwelling on September 29, 1944, showed notes about the nuclear project, and these, the FBI declared, "reflect an intimate knowledge concerning highly secret phases" of the project. Indeed, Adams was "the most dangerous espionage agent yet discovered in the Comintern Apparatus."[18] At Chicago's Development of Substitute Materials Laboratory, Hiskey assisted in plans for plutonium production. To get him away from Adams, the Army drafted Hiskey in April 1944, sending him to the Yukon as property survey master or, as an army official put it, to "count underwear." At this remote posting, more notes on the atomic project were discovered in his effects.[19]

Yet a more dangerous spy than Nelson, Adams, or Hiskey was Klaus Fuchs, whom the FBI entirely missed. From the Los Alamos Laboratory, he provided Moscow with unparalleled information about the bomb project, including material on such topics as its construction, detonation, and the fission rates of certain types of plutonium. He continued to spy for the Soviets from Britain when he returned there after the war. The Atomic Energy Commission declared that Fuchs's information likely sped up Soviet atomic research by two years. Though the physicist's intelligence gathering at Los Alamos remained unknown until 1950, defector Igor Gouzenko revealed another significant espionage operation less than a month after the war ended. A clerk at the Russian embassy in Ottawa, Gouzenko secreted out 109 documents that illuminated Soviet successes in obtaining atomic, radar, and other military-industrial secrets, which he showed to British and American officials. One of the most active sources Gouzenko named was Allan Nunn May, a Cambridge-trained nuclear physicist, who gave the Soviets "a survey of the entire atomic bomb project." May made three trips to the

Chicago laboratory, from which he transferred uranium samples to Soviet military intelligence in 1944.[20]

Gouzenko's was not the only high-profile defection of 1945. Elizabeth Bentley walked into the FBI's arms that fall as well. After some initial disbelief at her allegations of high-level espionage within the U.S. government, the Bureau assigned twenty-five agents to her case, launching technical and physical surveillance of the eighty-odd individuals she named. Her defection had the effect of a *Titanic*-sized iceberg on Soviet operations in the United States, as the Soviet security agency, then known as the NKGB, stopped all communication with a number of agents and recalled others. Bentley told the FBI about sources like Nathan Gregory Silvermaster and William Ullman, among many additional spies, who supplied her with reams of material from the Pentagon and other departments beginning in 1941, much of it photographed in Silvermaster's basement.[21] Soviet cables, which identified her as "Good Girl," confirm this mass quantity; the material streamed in, on planes, munitions, and manpower, dwarfing the limited take of Chambers's earlier sources.[22] Unfortunately for the FBI, her testimony as an uncorroborated witness had very little value for prosecution purposes. Only one man, War Production Board staffer William Walter Remington, testified that he had given information to Bentley, and he claimed that he thought she was merely a journalist. Everyone else denied her charges or took the Fifth Amendment. Bentley sometimes exaggerated her story in ensuing congressional hearings, but the dearth of convictions does not reflect a lack of merit in her initial claims about Soviet espionage practices, which have been since demonstrated in both Soviet archives and American sources like VENONA.[23]

The government also had a hard time after the war prosecuting the atomic spies it had identified for the same reason. Released from his arctic purgatory, Hiskey claimed he had provided no secret information. Joseph Weinberg similarly denied his involvement in espionage, claiming he had never met Nelson or talked to him about the bomb. As for Nelson, he took the Fifth Amendment repeatedly. The wiretaps that confirmed these men's actual roles were not sufficient as courtroom evidence. Moreover, even where a willing eyewitness was available, espionage charges were difficult to prove. Whittaker Chambers, after waffling for some years about Alger Hiss's actual relationship with him, finally named Hiss as a former spy in 1948 after the latter tried to sue him for defaming Hiss as a communist. But the statute of limitations on Hiss's espionage had expired, and despite Chambers's possession of 1930s State Department documents connected with the former Foggy Bottom official, Hiss could only be charged with perjury for denying that he had known Chambers. Hiss served three and a half years in prison and the rest of his life trumpeting his innocence, garnering many believers.

The government did get significant help in identifying spies from the aforementioned VENONA project, the Army Security Agency's secret effort to decode wartime Soviet cables, although their secrecy and their hearsay nature prevented them from being of much value for legal purposes.[24] The first and only

"live" American spy to be caught by VENONA was Judith Coplon, a political analyst at the Justice Department, arrested in March 1949 as she was supplying material to her Soviet handler, Valentin Gubitchev. Her 25-year sentence was overturned on appeal, owing to the FBI's missteps, including wiretapping her communications with her attorney. More significant, though, in 1949 cryptanalyists decoded a World War II cable on "Fluctuations and the Efficiency of a Diffusion Plant, Part III," written by Klaus Fuchs.[25] He soon confessed his espionage to British authorities. After a massive FBI manhunt, agents found Fuchs's American courier, Harry Gold, but he did not initially cooperate until his interviewers fished out a map of Santa Fe from his closet.

His New Mexican adventures now evident, an abashed Gold broke down. He was charged with "conspiracy to commit espionage on behalf of the USSR" on May 23, 1950; he got a 30-year sentence for his illicit information gathering. His sources had included not only Fuchs but engineer Abraham Brothman, chemist Alfred Slack, and Los Alamos machinist David Greenglass. Greenglass, too, soon talked with authorities, recounting the role of his sister and brother-in-law, Ethel and Julius Rosenberg, in recruiting him. They, of course, never cooperated.

In 1951, a congressional committee declared that the espionage of Fuchs, Greenglass, and others had "advanced the Soviet atomic energy program by 18 months as a minimum . . . if war should come, Russia's ability to mount an atomic offensive against the West will be greatly increased." This dire outlook certainly helps explain the extraordinary severity of Julius and Ethel Rosenberg's sentences.[26] Physicist Theodore Hall, a much more important source who had spied at Los Alamos, was luckier. He escaped because corroborating evidence outside of the classified VENONA intercepts was not available. Hall fled to England, where he lived nearly another fifty years; he only publicly admitted his role in 1998.

Cryptanalysts also used VENONA to develop information about Julius Rosenberg's ring of engineers, including Joel Barr, Alfred Sarant, and William Perl. Sarant and Barr alone produced over 9,000 pages of documents on radar and other technology with military applications. Perl, meanwhile, was given a prize for the lode of aircraft information he furnished.[27] As soon as Gold and Greenglass were apprehended in 1950, Barr escaped to Czechoslovakia. Sarant fled there also, via Mexico. Another of Rosenberg's engineers, Morton Sobell, also left the United States for Mexico on the day of Greenglass's arrest. Seized by the Mexican police, Sobell resisted, but eventually had a ".38 caliber pistol butt" smashed on his head.[28] He ended up on trial with the Rosenbergs, named by his former friend and roommate, Max Elitcher; he got a 30-year sentence and served eighteen years, five of them at Alcatraz. This was certainly an unusually harsh penalty for industrial espionage. Sobell, who is still alive, has always denied his role in Rosenberg's ring.[29]

Perl, on the other hand, did not flee, but because officials had really only the secret VENONA materials as evidence against him, he could not be charged as a spy. Instead, he was convicted of perjury, for denying that he knew both Rosenberg and Sobell, his former classmates at City College, and received two

concurrent 5-year terms. Hoover, annoyed that Perl had not been charged with espionage, took cold comfort in his treatment at the New York Federal House of Detention, where the brilliant engineer was relegated to cleaning toilets.

The government didn't even get a perjury case against Steve Nelson. After the war, he was busy organizing immigrants in an unglamorous section of Pittsburgh. The House Un-American Activities Committee (HUAC), which was familiar with the FBI's wiretaps on Nelson, ordered him to appear in 1948 and 1949, but he refused to testify. Moreover, he flatly denied any role in espionage and continued to deny it for the rest of his life: "There may have been a Soviet espionage network operating in this country," Nelson wrote in 1981, "but common sense would dictate against recruiting prominent Party officials."[30] Congress charged him with contempt for his refusal to cooperate, but more troublesome for him was the Commonwealth of Pennsylvania's charge that he had violated a 1919 state sedition law. Authorities there sentenced him to twenty years in the ancient Blawnox workhouse, plus a fine of $20,000. After two appeals, he was finally vindicated by the U.S. Supreme Court in 1954; one could not be seditious to a state when the federal government had its own laws in the matter. Later in the decade, ironically, disgusted with Nikita Khrushchev's 1956 revelations about Josef Stalin, Nelson left the Communist Party.

By then, with only a few thousand members, this organization was riddled with FBI informants. Still, Hoover only planned to amplify his assault on the party through the COINTELPRO project. As one FBI staffer noted, "We were trying first to develop intelligence so we would know what they were doing [and] second, to contain the threat. . . . To stop the spread of communism, to stop the effectiveness of the Communist Party as a vehicle of Soviet intelligence, propaganda and agitation."[31] The 1956 COINTELPRO against the Communist Party proved such a successful model that the FBI set up similar efforts against organizations ranging from the Ku Klux Klan to the New Left in ensuing years.

The domestic party was unlikely to be doing much spying in the 1950s, of course, with the FBI's saturation of its ranks. Instead, Soviet agents bent on espionage focused increasingly on cultivating American spies overseas, especially men in uniform—an approach that proved successful throughout the Cold War and beyond. Of thirty-three U.S. espionage cases prosecuted between 1950 and 1975, fully twenty-three were either soldiers or civilians connected with the military abroad.[32] Though spy convictions abounded in the military sector, intelligence agency operatives who spied for Russia were seldom publicly revealed in this era. The CIA and the Justice Department had a pact, first signed in 1954, that allowed the intelligence agency to decide whether to send any of its agents suspected of illegal activities to Justice for prosecution. Not surprisingly, suspected personnel usually remained secret to the CIA for reasons of "national security."[33]

In 1957, the same year that the Soviet *Sputnik* satellite caught Americans off-guard, the United States was also surprised by a Russian spy living in Brooklyn, KGB illegal Rudolf Ivanovich Abel. Abel, who had been in the United States for almost ten years, was found guilty of conspiracy to obtain and transmit

defense-related information to the Soviet Union, as well as for being an unregistered foreign agent. Authorities were assisted in finding him by a defector, Reino Hayhanen, himself a former KGB spy, along with a newsboy's earlier puzzling find of a hollowed-out nickel containing a secret code. Abel (whose actual name was Willie Fisher) was sentenced to serve thirty years in prison. But in 1962, after U-2 pilot Francis Gary Powers was caught red-handed when his spy plane crashed in a Russian field, the United States let Abel go in exchange for the downed flyer.

In 1960, Powers's exposure led two disgusted Americans, National Security Agency (NSA) mathematicians Bernon F. Mitchell and William H. Martin, to defect to Russia with their cryptographic secrets. In a public attack from Moscow, Mitchell and Martin vilified American secret missions over Soviet airspace. HUAC, however, blamed the men's supposed homosexuality for their betrayal.[34] Another NSA employee who also spied in the early 1960s, Jack Dunlap, was never caught. After failing a polygraph test in 1963, Dunlap made several attempts to kill himself; he completed the deed before authorities could unearth what he had stolen from the NSA. The same year, even as Kennedy and Khrushchev signed a comprehensive atomic test-ban treaty, an Air Force employee was successfully apprehended for furnishing the KGB the secrets of the Strategic Air Command's communications technology. John Butenko received a 30-year sentence for his spying.

Unfortunately for the United States, efforts to recruit its own moles to penetrate Moscow's intelligence agencies in this era remained stillborn owing to the paranoia of James Jesus Angleton, head of the CIA's Counterintelligence Staff, who became convinced that working with Soviet double agents would only involve the CIA in a deceptive KGB "monster plot." Persuaded by a defector, Anatoly Golitsyn, that the agency had been already penetrated, Angleton's agency was hamstrung—and yet no mole was disinterred.

By the 1970s, the diplomatic environment of détente prevented much spy catching. Here the story of Valery I. Markelov is revealing. In 1970, Markelov, a UN KGB operative, met a Grumman engineer and told him that he was very interested in that company's F-14 fighter jet. The engineer then contacted the FBI, and the Bureau monitored the two men's meetings over the next two years; at their last meeting, in February 1972, the FBI arrested Markelov with confidential documents in his hands. Soon indicted for espionage, Markelov saw his indictment dismissed by the Nixon administration. Eager to use Moscow's assistance in extricating itself from Vietnam, it claimed letting him go "would best serve the national and foreign policy interests of the United States."[35]

By 1975, however, with the United States' ignominious rout from Vietnam and Communism seemingly on the march around the globe, the bloom had faded from the détente rose. That June, the FBI arrested Sarkis O. Paskalian, one-time director of performing arts at the Armenian General Benevolent Union and a longtime KGB agent, along with his cousin, Sadag K. Dedeyian, a former mathematician at the Johns Hopkins Applied Physics Laboratory, who had supplied Paskalian with information about NATO's strength. Paskalian was given a

22-year sentence, and Dedeyian, a three-year term. The arrests prompted FBI Director Clarence Kelley, sounding much like his predecessor Hoover, to declare that the United States was a "prime target" for Soviet intelligence collection.[36] In summer 1977, the FBI fought back with a so-called dangle operation, sending retiring Navy Lt. Cmdr. Art Lindberg to schmooze aboard the Soviet tourist vessel *Kazakhstan* en route to Bermuda. On the trip, Lindberg snared three men from the Soviet UN Mission who eagerly took his Navy-screened materials on anti-submarine warfare and advanced helicopters until the FBI arrested them in May 1978. Two were tried and sentenced to fifty years in prison, although they were later exchanged for five Soviet dissidents. Not all the spies arrested in this era were working for the Soviet Union, however; Ronald Humphrey of the U.S. Information Agency had earlier provided information to the North Vietnamese delegation at Paris, hoping to free his wife and family from the communists. Unfortunately for him, his go-between was a double agent under FBI supervision. Humphrey and an accomplice got a 15-year term.[37]

Another spy identified in the post-détente Carter administration was CIA official David Barnett, who for nearly $100,000 provided names of agents, materials on submarines and missiles, and other information to the KGB. He was sentenced to eighteen years in jail. As his treatment suggests, the CIA-Justice gag rule had been quashed; in the mid-1970s, Frank Church's (D-ID) Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, which was investigating intelligence agencies' abuses in the post-Watergate era, saw it as an abuse of executive power. President Gerald Ford thus axed the rule, but counterintelligence officials did not entirely drop their resistance to prosecution. When William Kampiles, a disgruntled CIA trainee, stole a top secret manual for a KH-11 military surveillance satellite in 1977 and sold it to the Soviets for $3,000, both the CIA and the Defense Department opposed his going on trial. The CIA was embarrassed by the laxity that Kampiles's espionage case would demonstrate, and the Pentagon worried about maintaining the secrecy of the satellite. As a result, the trial included closed sessions and limits on access to the material in question. Similar measures were employed in the prosecution of Christopher Boyce, a TRW employee who sold defense secrets from his firm to Moscow in 1977, and such provisions were enshrined in the Classified Information Procedures Act of 1980.

Boyce was one of the most famous spies arrested in this era, owing in part to Robert Lindsey's book about his case, *The Falcon and the Snowman* (1979). Though he earned $20,000 for his work, Boyce seems to have been motivated most by a strong disagreement with American foreign policy, especially its unequal relationship with client-states like Australia, which provided bases to support satellite intelligence collection without being furnished full data. Given a 40-year sentence, Boyce escaped from jail three years later—some believed he had been sprung by the KGB—and survived outside for almost two years, helped by a sympathetic woman friend. He hardly laid low; instead, he participated in sixteen bank robberies while on the lam. Upon capture, he got another

twenty-eight years tacked on to his prison term. Boyce initially showed little remorse for his actions, telling an Australian TV audience in 1983: "I think that eventually the United States Government is going to involve the world in the next world war. And being a traitor to that, I have absolutely no problems with that whatsoever."[38] After being beaten up by members of the Aryan Brotherhood at Leavenworth prison, he was transferred to solitary confinement at Marion, Illinois, the federal system's most secure lock-up. This experience seems to have sobered him, for in 1985 he told the Senate Select Committee on Intelligence that espionage was "pretty dirty business . . . it is not what you see on television." Spies, he noted, are "bringing down upon themselves heartache more heavy than a mountain. There is no exit from it."[39] Boyce was released in March 2003.

Not long after Boyce's arrest, lawmakers had authorized more controversial methods to catch even more spies. The Foreign Intelligence Surveillance Act of 1978 (FISA) allowed investigators to wiretap or otherwise secretly monitor suspected terrorists and espionage agents without worrying about violating the Fourth Amendment's protection of criminal defendants from unlawful search and seizure. Under this act, a panel of judges reviews the government's requests for surveillance and almost always accepts them: In 2004, for instance, the panel approved every one of the 1,758 requests put before it for secret surveillance (wiretap authorizations are somewhat more sparingly approved). The requests are much more frequent now than they were before September 11, 2001, not surprisingly. Just days after those attacks, in fact, Congress passed the USA-PATRIOT Act, which makes it even easier for the government to conduct surveillance on Americans and allows agencies to share the results of wiretaps and grand jury proceedings if they relate to foreign intelligence or counter-intelligence. Nevertheless, the Bush administration drew an outcry when it began monitoring foreign phone calls of some Americans without FISA authorization in late 2005.[40]

With measures like FISA and the Classified Information Procedures Act in place, the 1980s saw a huge expansion in the number of espionage practitioners apprehended; authorities arrested sixty-two of them in the oft-named decade of the spy. Given the high-profile American defense buildup of this era, it is not surprising that much of the Soviet espionage at this time focused on military technology. It included, for example, the theft of radar at Hughes Aircraft in Los Angeles, the swiping of materials on the Minuteman Missile from Systems Control in northern California, and the pilfering of Stealth airplane technology at Northrop Advanced Systems. Declared FBI Director William Webster in 1984, "We have more people charged with espionage right now than ever before in our history."[41] Though the FBI deserves credit for cracking these cases, a good number of them originated with the revelations of defectors.

Even the hallowed halls of Congress were not immune from espionage in the 1980s. Randy Miles Jeffries, a stenographic messenger with a history of heroin abuse, twice supplied top secret materials from closed hearings of the House Armed Services Committee to Soviet military officials. He was arrested in 1985

on his third effort and was sentenced to serve from three to nine years. Jeffries, in fact, was the twelfth person charged with espionage in 1985, "the year of the spy." Among those apprehended that year also was Jonathan J. Pollard, a naval analyst who spied for Israel and remains in solitary confinement twenty-one years later. The exact information Pollard provided remains classified but included material on U.S. signals surveillance practices. His sentence was unusually harsh, similar to that meted out to top Soviet spy Aldrich Ames. As recently as February 2006, Pollard's attorneys had filed for the release of documents that would assist in a clemency petition; Pollard has been rejected, though, in every one of his appeals.

Another spy identified in 1985 who also got a life sentence was NSA communications specialist Ronald Pelton. He furnished Moscow agents information about Operation Ivy Bells, a top secret Navy program in which U.S. submarines placed bugging devices on Soviet undersea cables. Famed KGB defector Vitaly Yurchenko brought him to the FBI's attention. Yurchenko also identified CIA agent Edward Lee Howard, whom the agency, now freed from Angleton's anxieties, had hired in 1981 for the delicate task of managing Russians cooperating with the CIA inside the Soviet Union. Yet Howard, like Jeffries, had a history of substance abuse. Once fired, he began passing crucial information to the KGB, resulting in the death of at least one American agent. He averted arrest by escaping to the Soviet Union, the first CIA employee to do so. He died in Russia in 2002.

The most significant spy arrest in 1985 was that of John A. Walker Jr. Walker had first betrayed highly sensitive Navy codes in 1967, when he was a debt-ridden submarine officer, an unhappily married man with four children to support. The Soviets paid him $4,000 a month. Walker left the service in 1976, realizing he would not pass a background check if his ex-wife were interviewed. By then, he had firmly established his network by recruiting his friend Jerry Whitworth, a naval communications specialist, who supplied much cryptographic material. Walker also turned to his family, where his most productive source was his son Michael, a sailor on the U.S.S. *Nimitz* who stole numerous burn bags of classified information before they hit the ship's incinerator. Walker's arrest, too, was a family affair: His ex-wife turned him in.

Before it was rolled up, the Walker ring had provided a vast amount of information, including the codes needed to start nuclear weapons in war, keylists that allowed the Soviets to read naval messages, and the Navy's plans for possible war in Central America. Yurchenko contended that Walker's ring represented "the most important operation in KGB history," even more so than the World War II efforts to acquire nuclear secrets.[42]

Despite the discoveries, some notable new espionage operations began in 1985. It was then that FBI agent Robert Hanssen greatly accelerated his espionage work. It was also in that year that Aldrich Ames of the CIA's Soviet counterintelligence branch launched his nine-year career in Soviet service. While missing Ames, the CIA did discover in the 1980s that its own espionage

operations in Cuba had been compromised for twenty years; all of its Cuban agents actually worked for the Direccion General de Intelligencia (DGI), Castro's secret service!

As these cases indicate, during an era of often tense Soviet-American relations, most of those charged with espionage worked for Moscow and its client-states. There were exceptions: In 1986, Michael H. Allen, a clerk at an American naval air station in the Philippines, stole classified documents that he handed over to the Manila government in exchange for assistance to his businesses, including a cockfighting enterprise. He got eight years in prison. Douglas Tsou, an FBI agent who had escaped from communist China in 1949, was arrested in 1986; he had spied for Taiwan and got a 10-year sentence. In 1988, Thomas J. Dolce received a similar prison term for spying for South Africa at the Aberdeen Proving Ground. At the same time, two Beijing diplomats, Hou Desheng, a military attaché, and Zang Weichu, a consular official, were tossed out of the country for trying to get NSA materials in an FBI sting operation. Similarly stung and chucked out was a Soviet military attaché, Yuri Pakhtusov, who had tried to get secret information from a defense contractor.[43]

The end of the Cold War drew an expanding range of countries into espionage against the United States. During the Gulf War in the early 1990s, Joseph G. Brown, a former member of the Air Force, was arrested for spying for the Filipino government, providing materials on Iraq as well as on the activities of insurgents in the islands. His material came from one of his karate students, a CIA secretary named Virginia Baynes. Indeed, it was the chance to become martial arts teacher at Langley that enticed Brown to return to the United States, where he was arrested as he deplaned in 1992; he got six months in jail. Meanwhile, Ronald Hoffman, an employee of Science Applications International, sold four different Japanese companies the software for designing missiles and identifying rockets from their exhaust trails and received more than $750,000. When his secretary discovered what he was doing, Hoffman quit his job, but then recklessly sneaked in after hours to get more material—and was recorded on camera. A government sting (which proffered the opportunity to sell the technology to South Africa) led to his arrest in June 1990, and he received a 30-month sentence for violating not only the Arms Export Control Act but the Comprehensive Anti-Apartheid Act, too.

This was relatively light compared to the thirty-four years at hard labor meted out to Army artillery specialist Albert Sombolay, who was apprehended the following year for offering his services to the Jordanians and Iraqis. Not all military personnel faced such a stiff sentence for spying for Middle Eastern governments. U.S. Navy Lt. Cmdr. Michael S. Schwartz had passed classified material to the Saudi navy in the early 1990s while stationed in Riyadh. Arrested in May 1995, he professed to have done it in a zealous attempt to assist Saudi—U.S. relations during the Gulf War. He avoided jail, suffering only the loss of military benefits.

The fall of the Berlin Wall also allowed U.S. authorities to discover spies for the defunct East Bloc. One of these, Jeffrey Carney, a former Air Force

intelligence operative, had spied for East Germany since the early 1980s, defecting there in 1985. He continued to work for the Stasi on the other side, and was arrested in 1991 when the security service archive was opened; he was sentenced to thirty-eight years in prison, later reduced to twenty years. Another, more significant East Bloc case was the Lee Conrad spy ring, first cracked in 1988. Conrad, a U.S. Army sergeant in Germany, sold secrets to the Soviet bloc for thirteen years. Members of his extensive ring included Kelly Therese Warren, a secretary in the 8th Infantry Division headquarters in Germany. Arrested in 1997, she provided material to Conrad for Hungary, including NATO plans for the defense of Western Europe in case of a Soviet attack. For the mere $7,000 she'd earned, she got a 25-year sentence.

As these cases suggest, the military continued to be a prime recruiting ground for spies. But it had no monopoly on illicit intelligence gathering. John Lalas was a State Department officer who spied for the Greek government for more than a decade and a half before he was arrested in Virginia in 1993, after he had provided over 700 documents to Athens on everything from military strategy to the names of CIA agents. The United States was tipped off by the comments of a Greek embassy official, and Lalas got a 14-year sentence. Another State Department officer, Geneva Jones, was also arrested in 1993. With a top-secret clearance in the Bureau of Politico-Military Affairs, she gave thousands of secret State Department cables, mostly related to Somalia and Iraq, to a West African journalist named Dominic Ntube. The materials appeared in African magazines and got as far as the hideout of Liberian rebel leader Charles Taylor. She received a sentence of 37 months in prison for sneaking out documents (which she had wrapped up in grocery bags and newspaper) and "the unlawful communication of national defense information," a violation of the Espionage Act.

Government and military employees, though predominant, are hardly the only practitioners of espionage. Foreigners resident in the United States—like Jacob Golos, Andrei Shevchenko, and Arthur Adams earlier—still do their share. In 1993, an FBI sting caught Yen Men Kao, who along with other Chinese had tried to buy military technology that was illegal to export, including jet engines, jet radar, and plans for a Navy torpedo. He was deported, but not prosecuted, in the interest of preserving Beijing–Washington relations, leaving behind his family and two Chinese restaurants.

But certainly the most damaging clandestine information sharing in recent years has been carried out by employees of the nation's intelligence agencies—no surprise, given their privileged access. As head of the CIA's counterintelligence service in Europe, Aldrich Ames was officially charged with closely scrutinizing Soviet activities, and thus it is hard to think of a more valuable source for the Kremlin. He is reputed to have destroyed more than 100 U.S. anti-Soviet operations, as well as contributed to the deaths of 10 agents. The deaths were not hard to miss, and the CIA began a major effort to find their mole, soliciting the FBI's help for the first time. For too long, however, Ames's grandiose life style, supported by the $2.7 million he received from the Soviets, went unsuspected.

Finally nabbed in 1994, Ames got a life sentence with no chance of parole. His wife, Rosario, received five years for collaborating with him. Though the CIA fumbled here, the FBI itself took hundreds of agents out of counterintelligence operations in the late and post–Cold War era, deploying them instead in the fight against new threats such as drug-inspired violence. Such a focus allowed Soviet spies like Robert Hanssen to operate for years unsuspected within the Bureau.

The Ames arrest did spur Congress to pass the Violent Crime Control and Law Enforcement Act, which restored the death penalty for spying under certain conditions, including passing materials that resulted in the death of a U.S. agent. It also removed the 10-year statute of limitations on espionage. The Rosenbergs remain the only convicted U.S. spies to be executed, however. Prosecutors know that dead spies don't talk, and they have been loath to give up the opportunity to unearth details from them.

The new law allowed for the apprehending of espionage agents who had not been active for decades. In February 1996, the FBI arrested Robert Stephan Lipka in Millersville, Pennsylvania, after he was identified by Vasili Mitrokhin. As a 19-year-old NSA clerk thirty years earlier, Lipka had provided documents on communications intelligence to the Soviet Union and earned $27,000. With no statute of limitations in effect, Lipka received an 18-year sentence for this youthful malfeasance. A rather more impressive catch that year was Harold James Nicholson, former branch chief of the CIA's Counter-Terrorism Center, still the highest ranked CIA operative to be arrested. Between 1994 and 1996, he provided identities of CIA agents and sources, as well as everything else he could get from the CIA's secret computers. Nicholson agreed to cooperate, and his jail term was negotiated to 23½ years.

Though Jonathan Pollard remains the most famous, numerous spies have worked for allies of the United States, including Robert Chaegun Kim, a computer whiz at the Navy, arrested in 1996 for passing a large amount of classified military-intelligence material to South Korean naval attaché Baek Dong-Il. Kim, who apparently operated out of loyalty to his home country, got a 9-year sentence. Another man who attempted to spy for a friendly country was Jean-Philippe Wispelaere, who worked for the Australian Defense Intelligence organization, where he had access to highly classified U.S. materials derived from satellite spying. In 1999, he quit his job and tried to sell documents to the Singapore embassy in Thailand, whose staff told U.S. officials, enabling them to catch him in a sting. Flying into Dulles to receive his expected payment, he was arrested and ended up with a 15-year sentence.

Perhaps one of the more ambitious spy operations in the 1990s was orchestrated by Fidel Castro's government, itself the historic target of U.S. intelligence agents' sometimes obsessive plotting. Under the leadership of Cuban intelligence, the Red Wasp network, led by Gerardo Hernandez, infiltrated anti-Castro groups in Florida as well as U.S. defense installations like the Boca Chica Naval Air Station in Key West, in part to thwart possible U.S. attacks on Cuba. The group, which included both Cubans and Cuban Americans, was arrested in 1998;

three of the men got life sentences, though no secret information ever got back to Castro.

As this and other cases confirm, national loyalty continues to play a role in motivating spies. So, too, does ideology, as the case of Kurt Stand and his wife, Therese Marie Squillacote, suggests. Stand, a labor functionary, and his wife, who worked at the Department of Defense, were arrested with their friend James Clark in 1997 for spying for Russia and East Germany. Stand had been a spy for East Germany for twenty-five years, beginning in the early 1970s; all three had been leftist activists, even communists. Squillacote, who began her spying in 1980, indeed saw it as an "anti-imperialist" activity. Despite their political leanings, Stand earned $25,000. The FBI discovered them after Squillacote tried to offer her services to the South African Communist Party in 1995; the couple got lengthy sentences four years later.

Many Americans were eager to spy for the East Bloc, both within and without the United States, and Russian diplomats continued to assist in this task. In December 1999, the FBI found and arrested Stanislav Gusev dawdling in front of the State Department. Gusev, an attaché at the Russian embassy, was remotely controlling a listening device that had been secretly installed in a seventh-floor conference room down the hall from the offices of Secretary of State Madeleine Albright. Paul Redmond, former head of counterintelligence at the CIA, was surprised by this evidence of interest in State Department meetings, because the United States and Russia were no longer enemies. He thought that technology would be a better target for them: "If I were in Moscow, what I'd want to know is what's Microsoft going to do? What's Sun going to do?"[44]

Overall, however, it was Americans, not Russians like Gusev, who did the most damage. The well-publicized arrest of Robert Hanssen in 2001 capped a 15-year hunt for an agent who was responsible for the deaths of numerous U.S. sources in Russia, and who had sent thousands of documents to that country over a 22-year career in espionage, earning $600,000 in cash. Hanssen was the supervisor of the FBI's intelligence division—a perfect place to prevent himself from being discovered. He handed over extensive U.S. analyses on such subjects as Soviet nuclear strength and the American ability to withstand a nuclear attack, as well as top secret documents on U.S. intelligence activity, from satellites to radar to a prospective tunnel under the new Soviet embassy in Washington. He also supplied Moscow with the identities of fifty sources, several of whom were executed because of his betrayal, including one of the United States' most important agents, Dmitri Fedorovich Polyakov, or TOPHAT, executed in 1988. The government paid well to seal Hanssen's fate; the defector who produced crucial evidence in the case—including a garbage bag of documents with Hanssen's fingerprints—received $7 million and a new life in the United States. This generous remuneration was a far cry from the agency's bungling treatment of Krivitsky sixty years earlier. Hanssen was sentenced to life without parole in 2002.

Despite the fame of Hanssen, Russia has hardly been the only nation interested in American military technology in recent years. Peter H. Lee, a physicist at

Los Alamos, provided secret nuclear information in lectures to Chinese scientists during a 1985 visit to the PRC. Over a decade later, when he worked at TRW, he made another trip to China and provided more information about his work. He confessed in 1998 and got one year in prison, as well as 3,000 hours of community service. But when another Chinese physicist at Los Alamos named Lee was arrested in 1999, it turned out to be an embarrassing mistake. The FBI had learned that the Beijing government had obtained information about a highly advanced atomic weapon, a miniaturized warhead called the W-88, and suspicion fell on Wen Ho Lee, whose downloading of classified documents onto his own computer and associations with suspected spies had also drawn their suspicion. Lee, however, claimed he was innocent. He was nevertheless placed in solitary confinement for nearly a year, partly based on false information. When the case began to fall apart, Lee was freed in return for agreeing to a lesser charge rather than espionage. This blunder, along with the Hanssen debacle, contributed to the resignation of FBI director Louis Freeh.

The FBI's stumbles here, of course, paled in comparison to the intelligence community's shock at the terrorist attacks of September 11, 2001, a catastrophe that is still being dissected. The attacks, too, had a significant impact on the fate of accused spies who had nothing to do with these events. Caught before the attacks early in 2001, Hanssen's case never went to trial; his lawyers, like Ames's, plea bargained for him. By contrast, Brian P. Regan, a National Reconnaissance Office employee who was arrested in August 2001 for offering to sell information to Iraq, China, and Libya, did go on trial, where he faced the very real possibility of the death penalty. As legal analyst John Parry noted at the time, "Giving things to the Russians is bad, but not threatening in the same way as giving things to irrational terrorists." Defense lawyers, however, argued that a letter to Saddam Hussein found on Regan's computer was part of his "fantasy" of espionage rather than evidence of genuine spying. Regan's lawyers got him life in prison. Five months later, his effort seemed less of a fantasy when shovel-wielding FBI employees unearthed 20,000 pages of documents, as well as CD-ROMS and videotapes, that Regan had buried in nineteen different digs in two state parks in Virginia and Maryland.[45]

Another case affected by the post–September 11 environment demonstrated, too, that ideology has not died as a motive in espionage, despite the typical cash basis of the practice. That very September, authorities apprehended Ana Belen Montes, a Defense Intelligence Agency Cuban analyst who had spied for Cuba since 1985. She pled guilty to espionage in March 2002, her work based inspired by her beliefs "that U.S. policy does not afford Cubans respect, tolerance and understanding." Montes was sentenced to twenty-five years in prison.[46]

Although espionage is normally associated with governmental or military intelligence gathering, in the post–Cold War era Americans grew increasingly alarmed about commercial spying as well. "The threat of economic and industrial espionage looms over the horizon of the business world like a gray cloud threatening a placid sea," warned Congresswoman Ileana Ros-Lehtinen (R-FL)

in 2000.[47] Congress had already taken action, passing the Economic Espionage Act in 1996. Within two years, the FBI had 700 economic espionage investigations in process; each field office, moreover, had a white-collar crime section to address this issue. Though some of the more notorious cases tried under this act involved foreign firms illicitly collecting American technology, most economic espionage continues to be conducted by employees.

One of the first cases tried under this law involved a Taiwanese firm, Yuen Foong Paper Manufacturing, in 1997, which had tried to gain technology for a treatment of ovarian cancer from Bristol-Myers Squibb. In a second case, also in 1997, another Taiwanese company, Four Pillars Enterprises, was discovered to have paid an employee of Avery Dennison for adhesive technology for nearly a decade, costing the company $50 million. But a recent case is more typical. In December 2005, Suibin Zhang, an ex-employee of Netgear, a Silicon Valley software company, was charged with stealing secrets from one of his former firm's vendors and providing them to his new employer across the Valley. He faces up to ten years in prison if convicted.

Despite the post-9/11 tightened security environment, military espionage cases have hardly disappeared in recent years. Indeed, this period has created a new enemy and potential perpetrator of espionage: Al Qaeda. In 2004, Ryan Anderson of the Washington State National Guard was arrested in an FBI sting operation for trying to sell military secrets to men he thought were Al Qaeda operatives, including information on how to kill his fellow soldiers inside Humvees. He had been discovered in an Islamic Internet chat room by another citizen monitoring these communications, on the eve of his guard unit's departure for Iraq in late 2003. His defense lawyers asserted that he was both autistic and manic depressive, but he still received a life prison term.

Along with the prospect of new enemies, old allies continue to spy on the United States. In October 2005, Leandro Aragoncillo, a member of Vice President Dick Cheney's staff, sent White House and FBI secret records to Filipino associates plotting a coup. The case's origination in the White House was notable, as the executive mansion has generally been free of spies. During that same month, the U.S. charged a Defense Department official, Lawrence A. Franklin, with spying for Israel. Franklin had provided secret materials to the American Israel Public Affairs Committee (AIPAC) as well as to an Israeli diplomat in hopes they would use it to affect U.S. policy. In a startling move, the government charged his AIPAC contacts with violating the Espionage Act because of their "unauthorized retention and transmission of national defense information." The lobbyists to whom Franklin spoke, Steven Rosen and Keith Weissman, are the first two people outside the government to be so indicted. A former Justice Department official, Viet D. Dinh, who himself assisted in drafting the USA-PATRIOT Act, condemned this action, declaring that it "presents a novel case because the listener has no [evidence] for knowing what relates to national defense."[48] Perhaps it is not so novel, considering how many were prosecuted for violating the espionage act in World War I for doing even less.

In sum, by the early twenty-first century, spies are drawing their motivation from more varied sources than ever, from political and ideological sympathies to nationalist inclinations to commercial gain. The countries involved are similarly diverse. Though the FBI no longer sees espionage as the country's "biggest threat," it is still the agency's second priority, after terrorism, as the Bureau's website indicates. No doubt only more unexpected challenges and crises await, and catching spies, especially in defense-related areas, is likely to remain a key government concern.[49]

NOTES

1. Whittaker Chambers, "Unpublished Ms. of 1938 on Soviet Espionage," in Sam Tanenhaus Papers, box 25, Herbert Hoover Institute on War, Revolution, and Peace, Stanford, CA.

2. Dwight Eisenhower, *Crusade in Europe* (Garden City, N.Y., 1948), 32, quoted in U.S. Army Intelligence Center, *History of the Counter Intelligence Corps: The Counter Intelligence Corps Between the World Wars, 1918–1941* (Fort Holabird, MD: U.S. Army Intelligence Center, 1960), 96.

3. Editorial Comment on Fish Committee Report, 88, Rossiskii Gosudarstvennyi Arkhiv Ekonomiki (Russian State Archive of the Economy), *fond* 413, *op*. 13, *del*. 101, Moscow; see also "Still the Fish Committee Nonsense!" ACLU pamphlet, May 1932, available at http://www.debs.indstate.edu/a505s75_1932.pdf.

4. Hoover to Attorney General, January 2, 1932, cited in Frank J. Rafalko, ed., *A Counterintelligence Reader,* Volume I: *American Revolution to World War II* (Washington: National Counterintelligence Center, 1996), 159.

5. Quoted in Raymond J. Batvinis, " 'In the Beginning' . . . An Investigation of the Development of the Federal Bureau of Investigation's Counterintelligence Program, 1936 to 1941" (Ph.D. dissertation, Catholic University, 2001), 46.

6. Quoted in Max Lowenthal, *The Federal Bureau of Investigatîon* (Westport, CT: Greenwood, 1950), 425. In 1940, he chided Military Intelligence as having "crossed into matters upon which this Bureau has already been conducting investigations." See Hoover to Roosevelt, June 3, 1940, Official File 10B, box 11, Franklin D. Roosevelt Library, Hyde Park, NY.

7. Hoover speaking at the American Legion's Annual Convention in San Francisco, September 30, 1946, American Civil Liberties Union Papers, file 2731, reel 235, Seeley Mudd Library, Princeton University, Princeton, NJ. These inroads were significantly reduced thereafter; from a height of 80,000 members during the war, the number of party members shrank by the late 1950s to about 3,000, in large part owing to FBI harassment and infiltration of the party.

8. Athan Theoharis, *Chasing Spies: How the FBI Failed in Counterintelligence but Promoted the Politics of McCarthyism in the Cold War Years* (Chicago: Ivan R. Dee, 2002), 34.

9. See Ralph D. Toledano and Victor Lasky, *Seeds of Treason: The True Story of the Hiss-Chambers Tragedy* (New York: Funk and Wagnalls, 1950), 131. As FBI special agent Robert Thelan noted, "According to the surveillance logs of this case, Bentley, on two occasions, was surveilled . . . when she went to Penn Station and entered the ladies

rest room there and the surveillance was lost." Perhaps the FBI should have hired some female agents!

10. See Gary Kern, *A Death in Washington: Walter G. Krivitsky and the Stalin Terror* (New York: Enigma Books, 2003). His appeal to extend his visa—"the Soviet Government . . . would take measures to finish me off"—did not spare him for long.

11. Report of the Director of the FBI for the Fiscal Year 1945, 6. Report supplied to author by John Fox.

12. On the surveillance of Nelson, see D. M. Ladd to the Director, April 16, 1943, Re: Communist Infiltration of Radiation Laboratories (CINRAD), FBI File 100-16847-201; Communist Infiltration of Radiation Laboratory, University of California, Berkeley, California, FBI File 100-16980, July 7, 1943, 1; FBI Steve Nelson File, August 20, 1945, 100-16847-NR, 8–20 passim. The FBI files used here come from either the FBI's Reading Room in Washington, DC, or originated in Freedom of Information Act requests by the author.

13. Pash to Lansdale, June 29, 1943, cited in U.S. Atomic Energy Commission, *In the Matter of J. Robert Oppenheimer: Transcript of Hearing before Personnel Security Board and Texts of Principal Documents and Letters* (Cambridge, MA: MIT Press, 1971), 822. Also see surveillance on Oppenheimer in Julius Robert Oppenheimer, February 17, 1947, FBI background, attached to Hoover to Vaughan, February 28, 1947, President's Secretary File (PSF), box 167, Harry S Truman Library, Independence, MO.

14. On his party membership, see FBI letter to David Lilienthal, April 23, 1947, and memo, April 21, 1947, cited in Jerrold and Leona Schecter, *Sacred Secrets: How Soviet Intelligence Operations Changed American History* (Washington, DC: Brassey's, 2002), appendix 1. Berkeley professor Haakon Chevalier reported his and Oppenheimer's membership in the same unit of the party from 1938 to 1942. See Chevalier to Oppenheimer, July 13, 1964, cited at http://www.brotherhoodofthebomb.com, the website for Gregg Herken's *Brotherhood of the Bomb*: *The Tangled Lives and Loyalties of Robert Oppenheimer, Ernest Lawrence, and Edward Teller* (New York: Henry Holt, 2002).

15. Report on J. R. Oppenheimer, February 5, 1950, Summary Brief on Fuchs, February 6, 1950, FBI Klaus Fuchs File 65-58805-1202, 3; Chevalier Conspiracy," Part II, Steve Nelson file, August 20, 1945, 100-16980, 36; Barton L. Bernstein, " 'In the Matter of J. Robert Oppenheimer,' " *Historical Studies in the Physical Sciences* 12, no. 2 (1982): 246.

16. Leona Franey testimony, *Soviet Espionage Activities in Connection with Jet Propulsion and Aircraft*, 81st Congress, 1st sess. (Washington, DC, 1949), 104–5, 127–28; see also references to Shevchenko's contacts in VENONA 705, New York to Moscow, May 18, 1943; VENONA 1151, New York to Moscow August 12, 1944; VENONA 1327, New York (signature unrecoverable) to Fitin, September 15, 1944; VENONA 1607—1608, Anton (Kvasnikov) to Viktor (Fitin), November 16, 1944. The VENONA files are at the National Archives, Washington, DC.

17. A. H. Belmont to D. M. Ladd, espionage memo, May 15, 1950, 5, available at http://foia.fbi.gov/VENONA/VENONA.pdf.

18. FBI Arthur Adams file, New York, June 20, 1950, 100-331280-715, 188, 433; San Francisco FBI Comintern Apparatus (COMRAP) Summary Report 100-203581-3702 for period covering March 29, 1943, to November 1, 1944, Dec. 15, 1944, 12. I am grateful to John Earl Haynes for a copy of this report.

19. U.S. Congress, Committee on Un-American Activities, *Report on Soviet Espionage Activities in Connection with the Atom Bomb*, cited in U.S. Congress, Joint Committee on Atomic Energy (JCAE), *Soviet Atomic Espionage*, 82nd Congress, 1st sess. (Washington, DC, 1951), 166.

20. FBI, "Soviet Espionage Activities," October 19, 1945, PSF FBI box 167, 8–9. May, who died in 2003, was sentenced to ten years at hard labor. He later moved to Ghana, where he taught physics and kept up with nuclear developments in Africa.

21. T. G. Spencer Report, FBI Silvermaster file 65-56402-220, 18–23. When the FBI explored the basement later, they discovered photoflood bulbs with attachments, the bellows of a camera, light reflectors, an enlarger, photographic developing equipment and fluids, pans, printing paper, drying frames, negatives, electric driers, photograph trimmings, and empty film cartons in the trash. See December 13, 1945, report in Silvermaster file, volume 7, 65-56402-234, 158–59.

22. See, for instance, VENONA 794–799, New York to Moscow, reporting Silvermaster's information, May 28, 1943.

23. Hayden Peake does an effective job of demolishing the claims of one of Bentley's accused, William H. Taylor, that she was substantially inaccurate. See Peake, Afterword, in Elizabeth Bentley, *Out of Bondage* (New York: Ivy Books, 1988), 237–47, as well as the FBI's own listing of her corroborating evidence in idem., appendix B. On the FBI's difficulties in proving her allegations of espionage, see Gary May, *Un-American Activities: The Trials of William Remington* (New York: Oxford University Press, 1994), 88–89. On her exaggerations, see, for instance, Kathryn S. Olmsted, *Red Spy Queen: A Biography of Elizabeth Bentley* (Chapel Hill: University of North Carolina Press, 2002), 162–63. For confirmation of her materials in Russian archives, see discussions in Allen Weinstein and Alexander Vassiliev, *The Haunted Wood: Soviet Espionage in America—The Stalin Era* (New York: Modern Library, 2000), chaps. 5, 10, 11; and Harvey Klehr, John Earl Haynes, and Fridrikh Igorevich Firsov, *The Secret World of American Communism* (New Haven, CT: Yale University Press, 1995), 309–17.

24. See Robert Louis Benson and Michael Warner, eds., *VENONA: Soviet Espionage and the American Response, 1939–1957* (Washington, DC: National Security Agency/Central Intelligence Agency, 1996), xxi–xxvii.

25. See Summary Brief on Fuchs and Gold, February 12, 1951, 65-58805-1494X, 53; Report, February 6, 1950, 65-58805-1202, 19. See, for example, VENONA message 850, Moscow to New York, June 15, 1944. A month later, the resident agent at the Soviet consulate recommended a $500 bonus for Fuchs.

26. JCAE, *Soviet Atomic Espionage*, 5.

27. On Perl's "highly valuable" contributions, see VENONA 154, Fitin (Moscow) to New York, February 16, 1945.

28. Ladd to Director, August 23, 1950, 100-2483-236. The Bureau gave no credit to the Mexican police in this manhunt, declaring that they "fall far short of the the standards of reliability which a case like this requires." Yet it was the security police to whom fell the task of arresting the highly combative Sobell and then driving the Sobell family nonstop 750 miles to Laredo—except for "abrupt stops" so that the "extremely" carsick female Sobells could relieve themselves. Legation, Mexico City office, to Director, April 4, 1951, 100-2483-991, 7–12.

29. See Sobell, *On Doing Time* (New York: Scribner's, 1974), passim, and Sobell's discussions of the VENONA releases and his role, available at http://www2.h-net.msu.edu/~diplo/Sobell.htm.

30. Steve Nelson, James R. Barrett, and Rob Ruck, *Steve Nelson: American Radical* (Pittsburgh: University of Pittsburgh Press, 1981), 294.

31. U.S. Senate, Select Committee to Study Government Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans; Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Book III, 94th Congress, 2nd sess. (Washington, DC, 1976), cited at http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIa.htm.

32. See discussion in Katherine L. Herbig and Martin F. Wiscoff, *Espionage Against the United States by American Citizens* (Monterey, CA: Defense Personnel Security Research Center, 2002), 7–8. A full list of U.S. espionage cases from 1945 to 1989 is in Nigel West, *Games of Intelligence: The Classified Conflict of International Espionage* (New York: Crown, 1989), 57–60.

33. See Griffin B. Bell with Ronald J. Ostrow, *Taking Care of the Law* (New York: William Morrow, 1982), 100–101.

34. James Bamford, *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization* (New York: Penguin Books, 1983), 177–96 passim. The two men, fed up with life in the socialist paradise, tried to return to the United States in the late 1970s but were not admitted.

35. "Espionage in the Defense Industry," available at http://www.fbi.gov/libref/historic/famcases/petrov/petrov.htm (this site gives Markelov the alias Sergei Viktorovich Petrov).

36. "2 Arrested by FBI on Spying Charges," *Washington Post*, June 28, 1975.

37. These and many of the recent cases discussed below are detailed at the Pentagon's Defense Security Service website, www.dss.mil/training/espionage/industry.htm.

38. See Court TV website at http://www.crimelibrary.com/terrorists_spies/spies/boyce_lee/8.html?sect=23.

39. Quoted in "The Falcon and the Fallout," *Los Angeles Times*, March 2, 2003.

40. See report of William E. Moschella, Assistant Attorney General, to Dennis Hastert, Speaker, House of Representatives, April 1, 2005, at http://www.fas.org/irp/agency/doj/fisa/2004rept.pdf; and the American Bar Association's condemnation of the Bush Administration's practices, available at http://www.abanews.org/docs/domsurvrecommendationfinal.pdf, just one of many protests.

41. "Engineer Is Held in Scheme to Sell Secrets," *New York Times*, December 19, 1984.

42. Yurchenko quoted in Pete Earley, *Family of Spies: Inside the John Walker Spy Ring* (New York: Bantam Books, 1988), 358. After defecting and sharing so much, Yurchenko then redefected to the KGB, who claimed he'd been "drugged and kidnapped by American agents." More likely, he was upset by his treatment by American intelligence officials.

43. Newspaper digests of these cases are available at www.dss.mil/training/espionage/industry.htm.

44. *Sixty Minutes*, February 1, 2000, available at http://www.cbsnews.com/stories/2000/01/31/60II/main155216.shtml.

45. "Spy Trial Opens, Death Penalty Result Possible," Associated Press, January 28, 2003; "Convicted Spy Accepts Life Sentence: Sudden Sentencing Deal Will Prevent Prosecution of Ex-Air Force Analyst's Wife," *Washington Post*, March 21, 2003. Bush identified the governments of Iraq, Iran, and North Korea as part of an "axis of evil" in his State of the Union Address, January 29, 2002.

46. Ronald Radosh, "Cuba's Top Spy," Frontpagemagazine.com; *Washington Post*, March 20, 2002; *Miami Herald,* October 16, 2002.

47. "Corporate and Industrial Espionage and Their Effects on American Competitiveness," Hearing before the Subcommittee on International Economic Policy and Trade of the Committee on International Relations House of Representatives, 106th Congress, 2nd sess., September 13, 2000 (Washington, DC, 2000), 1.

48. See *Secrecy News*, from the Federation of American Scientists Project on Government Secrecy, no. 26 (February 23, 2006), and *Washington Post*, February 14, 2006.

49. FBI website, available at http://www.fbi.gov/priorities/priorities.htm.

4

THE SUCCESSES AND FAILURES OF FBI COUNTERINTELLIGENCE

ATHAN THEOHARIS

RELYING ON DEPARTMENTAL CONTINGENCY FUNDS, ON June 29, 1908, Attorney General Charles Bonaparte established by executive order a special investigative force within the Department of Justice, the Bureau of Investigation (formally renamed the Federal Bureau of Investigation, FBI, in 1935). Bonaparte's decision in effect contravened recent congressional actions of 1907–1908 that first rejected the attorney general's request to fund a special agent task force and then barred the Justice Department from contracting for the services of Secret Service agents. Because his decision violated the intent of these actions (although the 1870 statute creating the Department of Justice authorized it to prosecute "and detect" federal crimes), Bonaparte was forced to assuage congressional concerns. During January 1909 testimony before a House Appropriations Subcommittee, the attorney general emphasized the need for such a force, stressed that it would only investigate violations of federal statutes, and pledged to monitor its operations closely to ensure that agents would not violate privacy rights or monitor political beliefs. The size of this agent force (thirty-four in 1909) and Bonaparte's assurances deterred congressional opposition. Congress nonetheless approved appropriations in 1909 confining the Bureau of Investigation to "detection and prosecution of crimes against the United States."

Congress revisited this restriction in 1910, empowering the newly created Bureau to conduct "such other investigations regarding official matters under the control of the Department of Justice as may be directed by the Attorney General." This more permissive standard was triggered by the enactment that year of the Mann (or White Slave Traffic) Act criminalizing the transportation of women across state lines "for the purpose of prostitution, or for any other immoral purpose." Not only had Congress thereby expanded the definition of interstate

commerce crimes but a numerically larger force would be required with agents stationed outside Washington, D.C., subject to the supervision not of the attorney general but the bureau director.[1]

The belated (April 1917) U.S. military involvement in World War I did not fundamentally change the Bureau's role as a law enforcement agency. Its wartime investigations focused on alien residents, prominent antiwar critics, and radical activists. Those targeted included Socialist Party officials Charles Schenck and Eugene Debs, leaders of the radical Industrial Workers of the World Union, Senator Robert LaFollette, social reformer and pacifist Jane Addams, black nationalist leader Marcus Garvey, prominent Irish nationalist Eamon de Valera, and the anti-British and pro-Irish Hearst press and *Chicago Tribune*. The Bureau's most controversial actions, however, involved the arrests of hundreds of suspected "slackers" in New York City in 1918 and the arrests of 6,000–10,000 citizens and alien residents during dragnet raids of January 1920, the so-called Palmer raids. All were law enforcement operations, initiated on the suspicion that the targeted subject had violated either the Espionage Act of 1917, the Conscription Act of 1917, or the alien radical deportation provisions of the 1917 and 1918 immigration acts.[2]

Subsequent revelations that in the postwar years Bureau agents intensively monitored political and labor union activities and even investigated members of Congress instrumental in triggering a congressional investigation of the involvement of senior Harding administration officials in the Teapot Dome scandal, led President Calvin Coolidge to dismiss Attorney General Harry Daugherty in 1924. Harlan Fiske Stone, Daugherty's successor, in turn fired Bureau Director William Burns and issued a series of orders to preclude future FBI abuses. These included banning wiretapping and restricting investigations to violations of federal statutes. Investigations of political activities, though scaled back, were not wholly abandoned. Bureau Director J. Edgar Hoover (Burns's successor) encouraged concerned citizens to continue reporting on such activities while the FBI's agents were to report such information as coming not from their investigations but "sources." Bureau files on organizations such as the American Civil Liberties Union and the Communist Party (for a time during the 1920s renamed the Workers Party) continued to be developed.[3]

The real shift in the FBI's role occurred in the mid-1930s when it began to conduct intelligence investigations having no direct law enforcement purpose. The catalyst to this new role stemmed from twin domestic and international crises: the Great Depression at home and the international policies of Nazi Germany and the Soviet Union. The devastating economic crisis of the Great Depression caused many Americans to question the nation's economic and political institutions with some joining fascist and communist movements. Concurrently, as "subversive" powers committed to furthering their own international goals, German and Soviet officials sought to recruit American fascists and communists to conduct espionage.

President Franklin Roosevelt accordingly turned to the FBI to neutralize this perceived foreign-directed security threat. In May 1934, in a one-time response,

the president directed the FBI to conduct "an intensive and confidential investigation of the [American] Nazi movement with emphasis on anti-American activities having any connection with German government officials." Then, in August 1936, he met with Hoover to discuss "the question of subversive activities in the United States, particularly Fascism and Communism." Roosevelt was particularly concerned that "some [domestic] organizations would probably attempt to cripple our war effort through sabotage." No U.S. agency was acquiring "general intelligence information" about such "subversive activities," Hoover responded but then claimed that a 1916 appropriation statute would provide the authority allowing the FBI to conduct such investigations at the request of the State Department. Roosevelt orally concurred while emphasizing the need for secrecy (for domestic political as much as for security reasons).[4]

The sensitivity of intelligence investigations (which lacked any law enforcement purpose) ultimately posed a bureaucratic problem for FBI officials, because the 1916 statute required a State Department request to trigger them. In response to FBI pressure, on June 26, 1939, Roosevelt assigned to the FBI and military and naval intelligence sole responsibility for all such investigations. Then, in a series of delimitation agreements concluded with military and naval intelligence in 1940–42, the FBI acquired a monopoly over all domestic intelligence investigations—with military and naval intelligence investigations confined to military personnel and base security (which would include weapons programs such as the Manhattan Project).[5] FBI officials also expanded authorized investigative techniques. To anticipate espionage and sabotage, Roosevelt secretly authorized FBI wiretapping in May 1940 during "national defense" investigations—even though the 1934 Communications Act banned wiretapping and the Supreme Court ruled in 1937 that this ban applied to federal agencies and in 1939 required the dismissal of any indictment based on evidence obtained through wiretaps. On his own, Hoover authorized FBI break-ins of targeted individuals and organizations to install microphones or photocopy records, a series of mail-opening programs (to intercept and open mail transiting through the United States from identified foreign countries), and the cooperation of telegraph and cable companies access to cable traffic involving thirteen identified foreign countries transiting to and from the United States.[6]

Roosevelt's concerns that German agents might seek to exploit anti-Yankee sentiments in Latin and South America also led him to expand the FBI's counterintelligence role. Dating from 1940, FBI officials worked out with William Stephenson, the head of the British Security Coordination (BSC) stationed in New York City, a liaison relationship to ensure that German agents active in Latin and South America would be closely monitored. Then, on June 24, 1940, Roosevelt authorized the FBI to conduct "foreign intelligence work in the Western Hemisphere on the request of the State Department." In response, Hoover created a Special Intelligence Service (SIS) with FBI agents assigned as "legal attachés" to U.S. diplomatic missions in the capitals of eighteen nations in the region. The combination of the FBI-BSC liaison program and the FBI's SIS led to

the detection during World War II of 832 German espionage agents, the apprehension of 336, and the shutting down of 24 clandestine radio stations used by German agents to communicate with Berlin and with other agents in Latin America.[7]

In contrast to its successful counterintelligence role in Latin and South America, FBI counterintelligence operations within the United States had mixed results—striking successes and major failures.

In 1938 FBI agents arrested Guenther Rumrich and three other members of a German-directed espionage ring operating out of New York City (although another fourteen co-conspirators escaped arrest by fleeing to Germany). Dating from 1927, German intelligence operatives had recruited German American citizens and German alien residents to infiltrate defense plants (particularly those engaged in airplane and ship construction) and the U.S. military to obtain information about U.S. military technology and tactics, defense planning, and shipping operations in the port of New York. The acquired information was then relayed to Germany through couriers who were either passengers or employed in the shipping industry. In June 1941, moreover, FBI agents successfully shut down another German espionage operation, headed by Frederick Duquesne and involving thirty-three citizens and resident agents, that sought to relay sensitive defense information to Germany through a shortwave radio station in Centerport, Long Island. And in an even more dramatic success, FBI agents in 1942 arrested two four-man teams of German saboteurs, one that had landed in Amagansett, Long Island, and the second in Jacksonville, Florida. These teams' purpose was to sabotage American transportation and industrial facilities along the East Coast, an aluminum plant in Tennessee, and locks on the Ohio River.

The FBI's successes in the Rumrich, Duquesne, and German saboteur cases resulted more from good luck than FBI investigative prowess. In the Rumrich case, the original lead came in September 1935 when a customs officer apprehended William Lonkowski (a German agent sent to the United States in 1927) when boarding the liner *Europa* with film strips and letters concealed in a violin case. Alerted to German espionage plans, FBI officials received a further break when Rumrich blatantly attempted to obtain blank American passport forms in February 1938. Interviewed by military intelligence agents, Rumrich admitted his role. Military intelligence thereupon referred the matter to the FBI, and, in return for leniency, Rumrich identified the other participants in this operation. In the Duquesne case, German intelligence operatives had pressured William Sebold (an American citizen of German descent), during a family visit to Germany, to serve as a spy. When returning to the United States, however, Sebold contacted the FBI and agreed to participate in an elaborate sting operation. FBI agents assisted him in setting up a shortwave radio station to relay to Germany information obtained by their recruited spies. The apprehension of the German saboteurs was equally fortuitous, the byproduct of the inadvertent discovery of the landing of one of the four-man saboteur teams by Coast Guardsman John Cullen, when patrolling the beach near Amagansett. The saboteurs claimed to be fishermen

and paid Cullen a bribe. Having overheard them speaking German, a suspicious Cullen returned the next morning to discover the equipment and uniforms that the four men had buried in the sand. He immediately brought this discovery to the attention of the FBI. In the interim one of the four saboteurs, George Dasch, fearing discovery, approached the FBI and told agents the cover names and possible contacts of the other members of his team and the second team that had landed in Florida.[8]

Ironically, the most serious security threat was posed not by a wartime adversary, Nazi Germany, but a wartime ally, the Soviet Union. The FBI, however, failed to discover the scope of Soviet espionage activities during the prewar and wartime years. Dating from the late 1930s and continuing after the United States and the Soviet Union became military allies in 1941, FBI agents closely monitored Soviet embassy and consular officials stationed in the United States (as well as Soviets assigned to the wartime Soviet Government Purchasing Commission) and high-level American Communist Party officials. The scope and intensity of this counterintelligence effort cannot be fully documented either because relevant FBI documents remain classified or when released are heavily redacted. At a minimum the FBI wiretapped the Soviet embassy, the headquarters of the American Communist Party, and a host of radical labor union and political organizations; bugged meetings that Soviet officials or American communists attended; intercepted the mail of communist officials and activists; and broke into the offices and residences of prominent American communists and other radical activists. In these efforts, FBI agents sought to uncover activities "detrimental to the national defense of the United States with respect to espionage, propaganda activities and otherwise."[9]

Nonetheless, despite the intensity of FBI counterintelligence operations, the Bureau's agents failed to uncover the involvement of American communists and Soviet officials in espionage during the World War II era. These included the pilfering of FBI files by Judith Coplon, a communist employed in the Department of Justice; the atomic espionage activities of David Greenglass and Theodore Hall; and the pilfering of classified information for delivery to the Soviets by two rings of communists employed in various wartime agencies, one headed by Victor Perlo and the second by Nathan Silvermaster.[10]

The FBI, it must be emphasized, had not been deterred from seeking to learn about Soviet and American communist espionage activities by a Roosevelt administration indifferent to the employment of communists and motivated to sustain U.S.–Soviet cooperation, or because of the priority of German counterintelligence operations. In fact, Attorneys General Robert Jackson and Francis Biddle approved all FBI requests to wiretap the Soviet embassyand Communist Party headquarters and identified communist and radical activists. Furthermore, dating from 1940, FBI officials assured the White House that they had the situation in hand. In a 1941 report, for example, FBI Director Hoover claimed that the FBI's "active and intensive [counterintelligence] operations are carried on in keeping under observation and constant study the operations of the German,

Italian, Soviet and Japanese Agents. . . . The identification of all major representatives of the Governments specified are known and their activities are under constant scrutiny." Earlier in 1940, Hoover reported that FBI agents were able to "maintain a careful check against the channels of communication, the sources of information, the methods of finance, and other data relative to" Soviet, German, French, and Italian agents.[11]

Hoover's 1940 and 1941 reports had been prepared at a time when the United States was neutral and when the Soviet Union and Germany still adhered to a 1939 nonaggression pact. FBI surveillance of Soviet officials and American communists, however, did not abate and instead intensified after the United States and the Soviet Union became allies following the Pearl Harbor attack. Indeed, in post-1941 reports to the White House, the FBI Director emphasized the possibility of Soviet (and communist) subversion. Yet the only information that he reported about Soviet officials and American communists involved their efforts to influence either U.S. policy toward the Soviet Union, individuals of Baltic or Eastern European descent, or congressional legislation. Alternatively, Hoover cited communist efforts to influence labor union, youth, and civil rights movements.[12] This total failure to uncover the reality of Soviet espionage is documented by a December 1944 report on FBI "espionage and counter-intelligence operations" having "ramifications within the United States" that only cited the actions of German agents or double agents.[13]

Two cases in particular highlight this counterintelligence failure. The first is a massive FBI investigation of planned Soviet espionage activities and the second is the response of senior FBI officials to the defection of Victor Kravchenko, a Soviet official employed in the Soviet Government Purchasing Commission.

Through a wiretap of Communist Party headquarters, FBI officials learned that Communist Party leader Earl Browder had alerted a West Coast Communist Party activist, Steve Nelson, about a forthcoming sensitive initiative. Bugging Nelson's residence in Oakland, California, FBI agents intercepted Nelson's meeting with Soviet embassy official Vassili Zubilin in April 1943, at which time Zubilin gave Nelson a large "sum of money" for the express "purpose of placing Communist Party members and agents in industries engaged in secret war production in the United States so that information could be obtained for transmittal to the Soviet Union." Thus alerted to a planned Soviet espionage operation involving the recruitment of American communists, FBI officials benefited further with the receipt in August 1943 of an anonymous letter to Hoover that identified by name a number of Soviet officials who were purportedly involved in espionage (some employed in the Soviet embassy and others in Soviet consulates, the Soviet trading company Amtorg, or the Government Purchasing Commission).

In response, Hoover ordered a massive FBI counterintelligence operation, code named COMRAP (Comintern Apparatus), one that had the advantage of focusing on identified Soviet and Communist Party officials. FBI agents followed these individuals and from them followed those with whom they were in contact,

eventually totaling forty-six. Lasting two years, the FBI's COMRAP investigation (which extended beyond physical surveillance to include the extensive use of wiretaps, bugs, break-ins, and mail opening) failed to uncover a single instance of Soviet or American communist espionage. Indeed, a December 1944 report summarizing the results of this investigation claimed only that the suspects had distributed "pro-Russian propaganda" through the media and communist front groups to "influence the people and Government of the United States toward acceptance of Soviet foreign policy," to recruit new Communist Party members, to "collect political information of value to the USSR," to "secure information of value to the [Communist] Party," and to promote "the employment of Communists in Government work."[14]

This failure raises questions about FBI counterintelligence capabilities. In part, FBI efforts were neutralized by the safeguards adopted by Soviet officials, as trained professionals, to avert discovery. Equally important, FBI agents had focused on prominent communist leaders and not low-level functionaries (some of whom had severed contact with the Communist Party). FBI agents even failed to follow up on what could have been a promising lead—their discovery, through monitoring one of the COMRAP suspects, Louise Bransten, of her December 1944 meeting in Washington, D.C. with Nathan Silvermaster and Charles Flato. Silvermaster at the time was the subject of a Hatch Act investigation (authorizing the dismissal of any federal employee who was a Communist Party member). FBI officials first learned of Silvermaster's role as head of one of two Soviet espionage rings (and Flato's role as a contributing member) in November 1945 with the defection of the courier for these two rings, Elizabeth Bentley.[15]

A second FBI counterintelligence failure involved defector Victor Kravchenko. Alerted in February 1944 to Kravchenko's pending defection (formally announced in April 1944), FBI officials obtained Roosevelt's and Attorney General Francis Biddle's unqualified authorization to pursue this matter. (Hoover had sought such assurances in light of the potential impact on U.S.–Soviet relations.) Meeting with Kravchenko in March 1944, FBI agents learned that he was willing to brief them about the "espionage activity of Soviet representatives in the United States," about other "illegal conspiracies" between Soviet representatives and U.S. defense firms, about the "activities" of Soviet intelligence agents in the United States, and about the organization and plans of the Soviet Communist Party and the NKVD (the predecessor to the KGB). In return for this information, Kravchenko demanded personal protection (including transportation to a safe hiding place and a permit to carry a gun) and limited financial support (namely, "no monetary worries for about a year and a half"). Hoover immediately briefed Biddle about Kravchenko's demands. The attorney general again authorized the FBI Director to proceed as he saw fit. Biddle had concurrently secured Secretary of State Cordell Hull's approval, because this defection could adversely affect already delicate U.S.–Soviet relations. At first hesitant Hull concurred, convinced that this was a "matter of internal security and might involve sabotage," could provide insights into "what the Russians were

doing here," and could serve as a "convenient card" that he could use "when he next conferred" with Soviet officials.[16]

FBI officials, however, failed to exploit this opportunity to learn about ongoing and planned Soviet espionage activities. Instead, they launched an intensive investigation of Kravchenko and those Americans whom he contacted (all prominent anticommunists), suspecting that he "may be an agent" of the NKVD and thus "part of a NKVD scheme to check on the Bureau's activities and attempt to lay some predication for possible embarrassment of the Bureau." In this investigation that lasted until 1945, FBI agents used wiretaps extensively, conducted break-ins, and opened the mail of Kravchenko and his American contacts, in addition to monitoring their activities closely.[17]

The FBI's counterintelligence failures in part resulted from the difficulty of anticipating espionage, but just as important was the essentially political criteria employed to target suspected subversives. In guidelines issued in September 1936, Hoover ordered FBI agents to target "Maritime Industry, Government affairs, steel industry, oil industry, newspaper field, clothing, garment and fur industry, general strike activities, Armed Forces, educational institutions, general activities—Communist and Affiliated Organizations, Fascists, Anti-Fascist movements, and activities in Organized Labor organizations." This focus on radical labor union and political activists was not revised after U.S. military involvement in World War II. Among those targeted were the radical American Youth Congress (during a 1942 break-in of the organization's New York headquarters FBI agents photocopied Eleanor Roosevelt's correspondence with its leaders); Mrs. Roosevelt's contacts with the International Student Association (another radical youth group); anti-Nazi refugees from Germany (Thomas Mann, Bertolt Brecht, Hanns Eisler, Ruth Berlau, Leonhard Frank, Berthold Viertel), suspect because of their Marxist political views; and communists employed in the Hollywood film industry (targeted in 1942 under a code-named COMPIC program). Ironically, the catalyst to the COMPIC investigation was Hollywood's production of antifascist and pro-Soviet films (such as *For Whom the Bell Tolls* and *Mission to Moscow*), confirming that FBI officials' underlying concern was that communists could influence the popular culture.[18]

The reality of Soviet espionage became publicly known with Elizabeth Bentley's congressional testimony in August 1948, with the congressional and grand jury testimony of another communist defector, Whittaker Chambers, in August/December 1948, with the arrest in March 1949 and subsequent trial of Judith Coplon, and with the arrest in 1950 and subsequent trial of the Rosenbergs.

These publicized Soviet espionage activities had occurred three to six years earlier in 1944–45 (with the exception of Coplon, who remained a government employee at the time of her arrest). During the resultant investigations and media exposés, however, no question was raised about a seeming FBI counterintelligence failure. The FBI instead was credited with having ensured the convictions of Coplon, Alger Hiss, and the Rosenbergs. And although Coplon's conviction was reversed on appeal, owing to the failure of FBI agents to have obtained a

warrant and to having wiretapped her, even this reversal did not raise questions about methods or capabilities. The debate over Soviet espionage operations instead centered on the actions of the Roosevelt and Truman administrations, with the main accusation leveled by McCarthyites that these administrations' "softness toward Communism" had enabled disloyal communists to obtain federal employment and had also hamstrung the FBI from uncovering Soviet espionage.

This public debate was misplaced. In reality, the Roosevelt and Truman administrations had given FBI officials wide latitude to conduct counterintelligence operations (with Roosevelt authorizing FBI intelligence investigations as early as 1936, in 1940 secretly authorizing "national defense" wiretapping, and in 1942, reaffirmed by Truman in 1947, authorizing FBI investigations to effect the dismissal of disloyal federal employees). Ironically, the very cases that raised public doubts about these Democratic administrations and that had fostered a positive assessment of the FBI's investigative prowess underscore the Bureau's counterintelligence deficiencies.

The Bentley case indirectly documents this. Her November 1945 detailed account of her role as a courier for two wartime Soviet espionage rings, whose members she identified, first alerted FBI officials to this wartime Soviet espionage operation. The participants in this conspiracy had been able to retain their governmental positions despite a government screening program instituted in 1942 to preclude the employment of disloyal employees. (Under this program, an individual could be denied employment or dismissed should the FBI have uncovered evidence of "a reasonable doubt as to his loyalty to the Government of the United States.") The head of one of these two rings, Nathan Silvermaster, had escaped a Hatch Act firing and, in addition, Bureau agents did not launch an investigation to ascertain his involvement in espionage when learning of his (and Flato's) meeting with Bransten in December 1944.

Based on Bentley's disclosures in November 1945, FBI officials launched a massive investigation of those she identified as Soviet agents. A special squad of 200 agents intensively investigated her claims (concurrently urging her to renew her contact with her Soviet handler, Anatoly Gorsky). And because their main objective was to identify those involved in a suspected, ongoing espionage operation, FBI agents were authorized to employ a series of illegal investigative techniques: wiretaps, break-ins, and mail opening. Nonetheless, as recorded in a March 1970 FBI memorandum, despite having investigated Bentley's charges "over and over again," agents were unable to "substantiate and corroborate" them. An October 1946 report to the Truman White House, following up on the flurry of reports based on Bentley's November 1945 allegations that Hoover had sent to Truman administration officials between November 1945 and March 1946, offers further documentation of this failure. FBI officials then lamely justified their inability to corroborate Bentley's charges as due to the "time element," the alleged conspiracy having dated "back several years." This report continued, "The facts are strong in many instances and circumstantial in others principally because of the disparity in time between the date of these activities

and the actual report of these activities to the authorities."[19] The FBI's "facts," however, only involved the confirmation that the accused individuals knew and met with each other, whether socially, at public meetings, or through correspondence—but not that they engaged in espionage.

In the final analysis, the FBI's failure was the product of bad luck:Soviet officials had been alerted to Bentley's defection by Kim Philby, a secret Soviet agent employed in British intelligence. Apprised by Philby of Bentley's defection, Soviet officials first ordered their operatives in New York and Washington to "cease immediately their connection with all persons known to Bentley in our work," "to warn the agents about Bentley's betrayal," and to return to Russia before they could be interviewed by the Bureau. The recruited American spies were also instructed to deny any involvement in espionage but to admit to having known Bentley because the FBI might already have observed such contact. Although the FBI had failed to confirm the involvement of those named by Bentley in espionage, Justice Department officials convened a grand jury in 1948 hoping to break one of the participants into admitting his involvement and implicating the others. This strategy failed; none of those identified by Bentley was indicted.[20]

FBI officials' immunity from critical scrutiny recurred in what was contemporaneously seen to be its most brilliant counterintelligence success—the uncovering of a Soviet conspiracy to steal atomic bomb secrets. At various times during 1950, FBI agents arrested the participants in this operation—Julius and Ethel Rosenberg, David Greenglass, Harry Gold, and Morton Sobell. Yet despite the fact that this espionage operation had occurred in 1944–45, no question was then raised about this after-the-fact apprehension or about how this conspiracy was belatedly uncovered.

The identification of the participants in this Soviet espionage operation was the consequence not of FBI investigative efforts but a wartime military intelligence program, subsequently code-named VENONA. Military intelligence first intercepted Soviet consular messages sent from New York and Washington to Moscow during the years 1940–48 and successfully deciphered them (with the important breakthrough occurring in 1949–50). Because Soviet operatives had assumed that their communications to Moscow could not be deciphered, their reports at times included background information about their sources, which enabled military and FBI officials to identify the recruits (Greenglass, Rosenberg, Gold) even though these consular messages concealed their identities through code names. The FBI's principal contribution to the resultant prosecution of the Rosenbergs involved pressuring Greenglass, Gold, and Max Elitcher to admit their own involvement and implicating the Rosenbergs and then developing circumstantial information that corroborated their testimony in specific instances.

Military intelligence was responsible for vetting the individuals employed in the Manhattan Project. Nonetheless, under the wartime delimitation agreements, the FBI should have alerted military intelligence officials about all information that FBI agents had developed about the potential disloyalty of any of the Manhattan Project's employees. In this case, the FBI's failure was secondary.

The intercepted VENONA messages, however, pinpoint a more serious FBI counterintelligence failure. In contrast to the Los Alamos project, where Julius Rosenberg's role was indirect (recruiting his brother-in-law David Greenglass, a military recruit assigned to Los Alamos), the VENONA messages confirm that Julius Rosenberg had personally stolen and in addition had recruited two others, Joel Barr and Alfred Sarant, employed in defense-related industries to steal information about sensitive military technology for transmission to the Soviets. The classified information pilfered by these three included information about radar systems, jet engine designs, analog fire-control computers, and the proximity fuse. Barr and Sarant copied and transmitted 9,000 pages of secret documents relating to over 100 weapons programs and the entire 12,000-page design for a U.S. jet fighter while Rosenberg provided the design for the proximity fuse. Military intelligence was again responsible for vetting individuals employed in defense industries, butin this case the FBI failed to follow up when Barr and Sarant switched jobs when denied an earlier clearance. At no time, moreover, did FBI officials authorize investigations to ascertain whether either Rosenberg or Barr had engaged in espionage even when discovering their employment in defense-related work.[21]

Portrayed as the crime of the century at the time, the Rosenberg case was not the sole known instance of Soviet atomic espionage. The deciphered VENONA messages also documented that Theodore Hall (and his friend Saville Sax, who served as his courier to the Soviets) had similarly provided the Soviets with atomic bomb secrets. FBI officials learned of Hall's and Sax's roles at the same time as the Rosenberg-Greenglass-Gold operation. Without assessing the significance of the information that Greenglass had provided the Soviets (he was only a high school graduate), Hall was a particularly valued recruit, having graduated from Harvard College with a degree in physics at the age of eighteen. On receipt of his submissions, Soviet officials in Moscow characterized them as of "great interest" and encouraged further submissions.

Alerted by military intelligence in 1950 to Hall's and Sax's espionage activities, FBI officials launched a massive investigation that included checking files on communist activities compiled during the 1930s and 1940s, breaking into their residences and opening their mail, and monitoring their contacts and activities in 1950–51. Then, in 1951 FBI agents conducted aggressive separate interviews of Hall and Sax, hoping to break one or both of them to admit to their past conduct and implicate the other. In these interviews, FBI agents asked questions based on the documentation of their activities in the deciphered Soviet consular messages. Unlike Greenglass, Gold, and Elitcher, however, both Sax and Hall denied any involvement in espionage. Sax, moreover, brazenly explained why he had traveled to Albuquerque in 1945 (planning to apply for admission to New Mexico University) or why he had visited the Soviet consular office in New York in 1944 (to assist relatives in the Soviet Union through Russian War Relief). Because FBI agents could not break Sax or Hall, this investigation was closed in 1952. "All outside leads have been exhausted,"an FBI

official reported, and the "only indication we have" of Hall's and Sax's "espionage activity" came from VENONA and such information "cannot be disseminated outside the Bureau."[22]

The Bentley, Rosenberg, and Hall cases were not the FBI's sole counterintelligence failures. Another case, highly publicized during the Cold War era, involved former State Department employee Alger Hiss, indicted in December 1948 on two counts of perjury (for denying to a federal grand jury having given classified State Department documents to a known communist, Whittaker Chambers, in 1938). FBI officials first learned of this espionage operation not when it occurred in 1936–38 but when Chambers in November–December 1948 produced State Department documents that he claimed Hiss had given him.

Prior to this dramatic development, FBI officials had failed, first in 1941 and then in 1946, to pursue potential leads that could have uncovered the Hiss–Chambers relationship. In May–August 1941, an FBI informer, Ludwig Lore, told FBI agents of Chambers's "OGPU [Soviet intelligence] Activities in the United States" and his supervision of approximately seventy Soviet agents, and specifically of Chambers's contacts with two "private secretaries to Assistant Secretaries of State" and with another secretary employed by "one of the high officials of the Department of Commerce." Lore claimed that Chambers had obtained from the Commerce Department secretary "all necessary statistical data" and from the State Department secretaries "two extra copies" of the Roosevelt administration's diplomatic correspondence, which they had typed. FBI agents subsequently interviewed Chambers, who admitted only to having been in contact with an "underground group" of federal employees (identifying twenty, including Hiss but no secretaries) whose purpose was to influence government policy. FBI agents did not press him on the differences between his account and that of Lore–Chambers having endorsed their conception of the threat: communist influence on New Deal policy.

Then, in 1946, pressured by an FBI agent about his knowledge of Hiss's activities (the FBI had launched an investigation of Hiss in 1945 based on the suspicion that he might have engaged in espionage, during the course of which Hiss's phone was tapped and his mail opened), Chambers only claimed that Hiss was "favorably impressed with the Communist movement." When the interviewing agent asked Chambers if he possessed any documentary evidence that Hiss had been a Communist Party member, Chambers responded that he did not and then emphasized that he had "never purposefully held out any information and had always been forthright in relaying any information that he had in which the Bureau had shown an interest."[23] Ironically, much like Hiss himself, FBI officials were blindsided when Chambers produced in November–December 1948 documentary evidence (typed and handwritten documents and microfilm copies of State Department documents), which he only then admitted to having acquired from Hiss in 1938.

The FBI's principal contribution to Hiss's indictment, moreover, stemmed from the grand jury testimony of an FBI expert that the typed documents

produced by Chambers had been typed on the same typewriter owned by the Hisses. A further FBI effort to enhance Chambers's credibility to the grand jury (essential because he had abruptly changed his grand jury testimony between October and December 1948, in October denying any knowledge of espionage activity and then in December claiming that Hiss had regularly given him State Department documents since 1936) involved an attempt to identify the individual (known to Chambers only as Felix) who in 1936–38 had photographed the classified documents that Chambers claimed to have received from his government sources. The result was a fiasco—an alleged Felix, Samuel Pelovitz, was produced in December 1948 as a grand jury witness. During his testimony, Pelovitz denied knowing Chambers or to having any photographic skills. Prosecutors then called Chambers who at first identified Pelovitz as Felix but recanted this identification when called back before the grand jury, lamely explaining that Felix was not Jewish, but Pelovitz was. The FBI had produced the wrong man; Pelovitz coincidentally was a former communist and had resided (but not in 1936–37) on the same street (Callow) and city (Baltimore) as Chambers's Felix.[24]

The Hiss case highlights the centrality of luck for FBI counterintelligence successes—in this instance the fact that a communist defector had since 1938 maintained what he described as a "life jacket." The limits of FBI capabilities are further highlighted by another seemingly successful FBI counterintelligence operation—the apprehension of Justice Department employee Judith Coplon as a Soviet spy.

As in the Rosenberg and Hall cases, Coplon's recruitment as a Soviet spy was discovered through the VENONA project. The deciphered messages confirmed that she had been recruited in 1944–45 at the time of her employment in the Department of Justice. Coplon, however, had escaped discovery of her disloyalty whether in 1944–45 or with the inception of the Federal Employee Loyalty Program in 1947. Having first learned of her disloyalty in 1949, FBI and senior Justice Department officials sought to ascertain whether she continued her espionage activities and to identify her Soviet contacts. In the course of this intelligence investigation, Bureau agents wiretapped both her office and home phones (and those of her parents in New York, with whom she frequently visited). Bureau and Justice Department officials eventually decided to launch a sting operation to ensure her conviction for espionage by making available to her carefully selected FBI records that would command her attention but would not compromise the nation's security. Coplon bit, and she was arrested in March 1949 when attempting to deliver twenty-eight FBI records to Valentin Gubitchev, a Soviet intelligence operative assigned to the United Nations staff in New York.

Coplon's attorney petitioned the court during her first trial, demanding the submission of the twenty-eight FBI reports as evidence. When the judge so ordered, FBI officials recommended dropping the case rather than honoring this order—claiming that their public release would harm the nation's security. Justice Department officials rebuffed this proposal. The released records, though

not harming the nation's security, proved deeply embarrassing to FBI officials—confirming that agents monitored political activities and wiretapped extensively (fifteen of the reports were based on wiretaps). Coplon's attorney immediately demanded a hearing to ascertain whether his client had been tapped, a motion that the U.S. attorney prosecuting the case successfully rebuffed as a "fishing expedition." In Coplon's second trial, however, the presiding judge honored the defense's motion for a pretrial hearing resulting in the disclosure that Coplon's office and home phones had been tapped, that the FBI agent who denied any knowledge as to whether Coplon's phone had been tapped had in fact routinely received the results of these wiretaps, and that FBI officials had ordered the destruction of the Coplon wiretap logs "in view of the imminence of her trial." The combination of the revelations about FBI wiretapping activities and the failure of arresting agents to have obtained a warrant ultimately led to her conviction being overturned on appeal.[25]

The Coplon case underscores the problem of attempting to convict individuals when evidence had been illegally obtained through a counterintelligence operation. FBI and Justice Department officials were unwilling to disclose (in this case as in the cases of Hall and Sax) how they had learned of Coplon's espionage activities (and thus the reasonableness of the wiretaps and the failure to obtain an advance warrant). To do so would have publicly compromised the VENONA program.

These Cold War internal security cases had far-reaching political ramifications, lending support to a McCarthyite politics that blamed the Roosevelt and Truman administrations for Soviet espionage successes. Significantly, the McCarthyites never attempted to ascertain the reality of the FBI's responsibility and that FBI officials had been accorded broad latitude by both presidents. Just as important, Soviet recruitment of ideologically motivated federal employees had been foreclosed by the late 1940s owing to the stricter standards governing federal employment instituted by Truman in March 1947 under the Federal Employee Loyalty Program. Henceforth, Soviet officials were compelled to rely on their own agents or to recruit sources based on greed, not ideology.

Soviet officials also employed "illegals," that is, individuals not assigned officially to Soviet consular or embassy offices. One such was Rudolf Abel, a colonel in the Soviet Union's intelligence service, the KGB, who entered the United States from Canada in November 1948 on a false passport. The KGB's resident agent in New York, Abel was uncovered in 1957 due to the defection of another Soviet illegal, Reino Hayhanen. Recalled to the Soviet Union, Hayhanen interrupted his return upon arriving in Paris in May 1957, approaching the U.S. consulate and then advising a CIA officer of his role as a Soviet agent and how he had entered the United States in 1952 under a false passport. In return for a promise of resettlement, Hayhanen described Soviet intelligence activities, identified one of his recruits (Roy Rhodes), and provided background information that eventually led to Abel's apprehension. Hayhanen did not know Abel's cover name or residence but remembered meeting him in a photo studio in Brooklyn.

Based on this lead, FBI officials launched an intensive investigation that eventually led to Abel's arrest on June 21, 1957. Tried and convicted, Abel was released in 1962 in return for the Soviets' release of captured U-2 pilot Francis Gary Powers.[26]

Luck and solid investigation had led to Abel's apprehension. The same combination led to FBI uncovering another Soviet espionage ring headed by retired naval communications officer John Walker Jr., who dating from 1968 had provided the Soviets with sensitive information relating to naval communications. Walker's motives for spying were strictly mercenary; he was quite conservative politically—indeed his political beliefs and background as a private investigator and businessman enabled him to receive security clearances. Walker, moreover, recruited his brother (Arthur), son (Richard), and a friend (Jerry Whitworth) to pilfer classified information. FBI agents uncovered Walker's espionage activities and those of his ring fortuitously in 1984—their first awareness of possible espionage derived from an anonymous letter (written by Whitworth) to the FBI's San Francisco office and then from reports to the FBI's Boston field office from Walker's former wife, Barbara, and daughter, Laura. FBI agents were at first unable to identify the writer of the San Francisco letter and did not immediately follow up on Barbara's and Laura's reports on Walker's espionage activities. An intrepid FBI supervisor finally acted on these reports, triggering an intensive investigation that culminated in the arrests in May 1985 and resulting conviction of John, Arthur, and Richard Walker and Jerry Whitworth.[27]

If the Abel and Walker cases highlight the importance of luck to FBI counterintelligence successes, the FBI's delayed apprehension of Aldrich Ames was primarily the responsibility of officials in the Central Intelligence Agency (CIA). A career CIA officer, Ames was appointed in 1983 the head of the Agency's counterintelligence branch on the Soviet Union and then in 1990 was assigned briefly to the Agency's Counterintelligence Center. Disillusioned with the Agency and motivated by greed, in 1985 Ames approached the Soviets to sell secret information, particularly identifying Soviet officials whom the CIA had recruited as double agents. He continued thereafter, in return for large sums of money, to identify other double agents as well as providing sensitive CIA records. Troubled by the deaths (or disappearances) of these sources, CIA officials suspected a mole, although they did not focus on Ames until 1992 and only sought FBI assistance in 1991 to uncover the suspected spy—having ignored Ames's extravagant life style, sloppy work habits, and excessive drinking. When finally given free rein, the FBI's intensive investigation (including wiretapping and bugging Ames's residence, monitoring his credit card bills and trash, and following him) resulted in his arrest on February 21, 1994, and conviction.[28]

FBI officials experienced similar embarrassment owing to their failure over a 21-year period to uncover another U.S. intelligence official who had also identified to the Soviets the Russians whom the FBI and CIA had recruited as double agents. This spy, Robert Hanssen, was employed in the FBI's counterintelligence

division. After joining the FBI in 1976, Hanssen was assigned to the Bureau's counterintelligence division in 1979 and then in 1983 to that division's Soviet analytical unit, where he had access to sensitive information about FBI counterintelligence programs, the identities of fifty recruited Soviet double agents, and thousands of pages of classified FBI, CIA, and NSA documents. Dating from 1979 he provided much of this information to the Soviets in return for large sums of cash and diamonds. As the result of the death of one of the FBI's recruited double agents in 1986, Bureau officials launched an investigation to identify the mole. Nonetheless, Hanssen escaped detection until late 2000, in part because of the precautions he had taken as a skilled counterintelligence officer (including not disclosing his identity to his Soviet contacts and successfully diverting attention from himself). His arrest on February 18, 2001, was the byproduct of the November 2000 defection of a Russian intelligence officer who, in return for a $7 million payment, delivered to U.S. intelligence the Russian file on Hanssen. This file contained a tape of Hanssen's conversation with a Soviet official (enabling FBI agents to identify his voice) and a bag that he had used to provide documents to the Soviets that contained his fingerprints. Until acquiring this file, FBI investigators had focused on a CIA officer, Brian Kelley, as the suspected mole.[29]

This narrative does not recount the totality of FBI counterintelligence operations. Because of continued classification restrictions, it is impossible to ascertain whether these and other known counterintelligence operations are representative.[30] Nonetheless, the known history of FBI counterintelligence successes and failures permits some qualified observations.

First, FBI failures were not due to incompetence but to the difficulty of identifying carefully trained spies (or, for that matter, terrorists) who had an obvious interest in precluding discovery of their plans. The cases cited herein highlight the importance of luck (most notably the defection of Soviet intelligence operatives). These cases further confirm the impossibility of achieving absolute security. This is highlighted by the recent FBI investigation of the sender(s) of anthrax letters in October–November 2001. Despite the intensity of an FBI investigation that to date has lasted four years, the sender or senders of the anthrax letters remain unidentified. This failure occurred even though FBI investigators had three advantages: first, they knew that such letters had been sent (and did not need to anticipate this possibility); second, whoever sent the letters had to have access to a lab and the expertise to weaponize anthrax; and third, FBI agents had the vastly expanded surveillance authority provided by the 2001 USA-PATRIOT Act.[31]

The Ames and Hanssen cases further confirm the unreasonableness of an expectation of absolute security. Despite the repressive character of Soviet society, and although Soviet intelligence officials closely vetted potential recruits to ensure their ideological loyalty and were not constrained by a need to respect due process or privacy rights, FBI and CIA officials were nonetheless able to recruit Soviet intelligence officers to betray their nation's secrets.

Second, this history highlights that FBI agents either focused on the wrong suspects, ignored tantalizing leads, or (in the Kravchenko case) made unwarranted assumptions. The objective of anticipating espionage inevitably led to a form of profiling where suspects were targeted based on their politics and associations. This suspicion drove the COMRAP investigation, and, more recently, underpinned a recommendation of FBI agent Kenneth Williams.

In a report of July 10, 2001, recommending that FBI headquarters launch a nationwide investigation focusing on Middle Eastern alien residents attending flight schools, Williams cited in particular an Al Qaeda sympathizer, Zakaria Soubra. Soubra had come to Williams's attention because of his public role in organizing demonstrations and meetings against U.S. and Israeli policy in the Middle East, his militant beliefs that the resort to violence in defense of Islam was justified, and his advocacy of a unitary Islamist state. When interviewing Soubra, Williams discerned in his apartment photographs of Osama bin Laden and Chechnyan *muhahedeen*. The FBI's subsequent (post-9/11) investigation of Soubra (and others whom Williams had identified in his July communication) uncovered no evidence that they either had advance knowledge of the September attacks or were co-conspirators. That radical political activism does not predict violence and that anticipating terrorism based on public political activities is nonpredictive is confirmed by Williams's failure to have identified Hani Hanjour as a prospective terrorist. Hanjour had, off and on over the previous five years, attended flight schools in the Phoenix area; but he was not a known public exponent of Islamist views. Yet on September 11, 2001, Hanjour (not Soubra) piloted one of the four commandeered jets, American Airline Flight 77, into the Pentagon.

The *President's Daily Brief* of August 6, 2001, captioned "Bin Ladin Determined to Strike in the US," provides further evidence of the limitations of basing counterintelligence investigations on political criteria. The final paragraph of this document reported that the FBI was "conducting approximately 70 full field investigations throughout the US that it considers Bin Ladin related." None of these investigations, however, involved any of the nineteen terrorists who engineered the 9/11 attack. A July 2, 2001, communication from the FBI's Counterintelligence Division to federal, state, and local law enforcement agencies warning of possible terrorist attacks by groups "aligned with or sympathetic to Usama Bin Ladin [an alternative spelling of the Al Qaeda leader's name, often used by the U.S. government]," moreover, starkly admitted that "the FBI has no information indicating a credible threat of terrorist attack in the United States."[32]

Political (and as well ethno-religious) profiling has serious limitations—and carries the additional risk that such investigations could lead to violations of civil liberties and privacy rights. Indeed, one byproduct of the FBI's counterintelligence investigations of the World War II and Cold War years was the acquisition of information about the political and personal conduct of suspected subversives. Although this information could not be used for legitimate prosecution or

national security purposes, FBI officials in time (on the strict condition that recipients not disclose their actions) purposefully disseminated this information to "reliable" reporters, members of Congress, and congressional committees for the purpose of "influencing public opinion." These covert, and extensive dissemination practices proved crucial to the promotion of a McCarthyite politics.[33]

NOTES

1. Willard B. Gatewood, *Theodore Roosevelt and the Art of Controversy: Episodes of the White House Years* (Baton Rouge: Louisiana State University Press, 1970), pp. 236–47, 249–54, 257–87; Vern Countryman, "The History of the FBI: Democracy's Development of a Secret Police," in Pat Watters and Stephen Gillers, eds., *Investigating the FBI* (Garden City, NY: Doubleday, 1973), pp. 33–38; Max Lowenthal, *The Federal Bureau of Investigation* (New York: William Sloane, 1950), pp. 3–17; Sanford Ungar, *FBI* (Boston: Atlantic Monthly/Little Brown, 1975), 38–41.

2. William Preston, *Aliens and Dissenters: Federal Suppression of Radicals, 1903–1933* (New York: Harper Torchbooks, 1966), pp. 6–7, 118–51, 208–38; Robert Murray, *Red Scare: A Study of National Hysteria, 1919–1920* (New York: McGraw-Hill, 1964), pp. 14, 18–32, 210–22; Charles McCormick, *Hopeless Cases: The Hunt for the Red Scare Terrorist Bombers* (Lanham, MD: University Press of America, 2005), pp. 14–141; Lowenthal, *Federal Bureau of Investigation*, pp. 24–35, 83–129, 147–98; Ungar, *FBI*, pp. 41–45; Curt Gentry, *J. Edgar Hoover: The Man and the Secrets* (New York: Norton, 1991), pp. 71–72, 79–105.

3. Athan Theoharis and John Stuart Cox, *The Boss: J. Edgar Hoover and the Great American Inquisition* (Philadelphia: Temple University Press, 1988), pp. 76–80, 82–86, 92–94; Gentry, *J. Edgar Hoover*, pp. 117–42; Ungar, *FBI*, pp. 45–49.

4. Ibid., Theoharis and Cox.

5. Ungar, *FBI*, p. 101; Theoharis and Cox, *The Boss*, pp. 148–54, 179–85.

6. Athan Theoharis, *Spying on Americans: Political Surveillance from Hoover to the Huston Plan* (Philadelphia: Temple University Press, 1978), pp. 97–99, 106, 125–26, 130; Gentry, *J. Edgar Hoover*, pp. 281–82.

7. Douglas Charles, " 'Before the Colonel Arrived': Hoover, Donovan, and the Origins of American Central Intelligence, 1940–41," *Intelligence and National Security* 20, no. 2 (June 2005), pp. 225–37; Leslie Rout and John Bratzel, *The Shadow War: German Espionage and United States Counterespionage in Latin America during World War II* (Frederick, MD: University Publications of America, 1986), pp. 29–40, 454–56; Thomas Troy, *Wild Bill and Intrepid: Donovan, Stephenson, and the Origins of CIA* (New Haven, CT: Yale University Press, 1996), pp. 33–40, 63–76; G. Greg Webb, "Intelligence Liaison Between the FBI and State, 1940–44," *Studies in Intelligence* 49, mo. 3 (2005), pp. 25, 29–38.

8. Athan Theoharis, *The FBI and American Democracy: A Brief, Critical History* (Lawrence: University Press of Kansas, 2004), pp. 50–52; Francis MacDonnell, *Insidious Foes: The Axis Fifth Column and the American Home Front* (New York: Oxford University Press, 1995), pp. 49–61, 127–28, 131–33.

9. Athan Theoharis, *Chasing Spies: How the FBI Failed in Counterintelligence But Promoted the Politics of McCarthyism in the Cold War Years* (Chicago: Ivan Dee, 2002), pp. 49–50, 56–94; Theoharis and Cox, *The Boss*, pp. 9–11, 13–15; Athan Theoharis, "A Creative and Aggressive FBI: The Victor Kravchenko Case," *Intelligence and National Security* 20, no. 2 (2005), pp. 324–28.

10. Not all Soviet espionage successes were the consequence of FBI counterintelligence failures. Under a 1943 delimitation agreement, military intelligence had exclusive responsibility for all personnel employed in the Manhattan Project. This agreement prohibited the FBI from initiating any investigation of "persons connected with the Atomic Bomb Project," although the FBI did have the responsibility of forwarding to military intelligence any information its agents had obtained in the course of other investigations. Katherine Sibley, *Red Spies in America: Stolen Secrets and the Dawn of the Cold War* (Lawrence: University Press of Kansas, 2004), p. 145.

11. Theoharis, *Chasing Spies*, pp. 60–61.

12. A representative sample of such FBI reports to the White House includes: Letters, Hoover to Watson, October 24, 1942, August 3, 1943, September 30, 1943, October 27, 1943, August 7, 1944, and December 28, 1944, OF 10-B; all in Franklin Roosevelt Presidential Library, Hyde Park, NY.

13. Letter, Hoover to Hopkins, December 22, 1944, and accompanying Quarterly Report on Espionage and Counterintelligence Activities Having United States Connections, November 1, 1944, OF 10 B, Roosevelt Library.

14. Theoharis, *Chasing Spies*, pp. 62—78.

15. Ibid., pp. 47–49, 77.

16. Theoharis, *Chasing Spies*, pp. 50–53.

17. Theoharis, "A Creative and Aggressive FBI," pp. 321–31.

18. Theoharis, *Chasing Spies*, pp. 57–60, 151–55; Theoharis and Cox, *The Boss*, pp. 13, 191–93; Alexander Stephen, *"Communazis": FBI Surveillance of German Emigre Writers* (New Haven, CT: Yale University Press, 2000), pp. 2, 20, 35–36, 43–45, 50, 67, 76–77, 85, 89, 117–29, 138, 190–99, 253–69, 271, 275–76.

19. Theoharis, *Chasing Spies*, pp. 42–43.

20. Theoharis, *Spying on Americans*, pp. 197–98; Theoharis, *Chasing Spies*, pp. 41–43, 54–55, 239–41; Allen Weinstein and Alexander Vassiliev, *The Haunted Wood: Soviet Espionage in America—The Stalin Era* (New York: Random House, 1999), pp. 103–7.

21. Theoharis, *Chasing Spies*, pp. 17–18, 31–32, 45–47, 81–83; Steven Usdin, "Tracking Julius Rosenberg's Lesser Known Associates," *Studies in Intelligence* 49, no. 3 (2005), pp. 13—19.

22. Theoharis, *Chasing Spies*, pp. 31–32, 81–84; Theoharis *The FBI and American Democracy*, pp. 84–85. The FBI's voluminous file on this investigation, FBI 65-59122, documents the intensity of the investigation of Hall and Sax; the 1952 decision to close this investigation is Memo, name deleted to Branigan, May 8, 1953, FBI 65-59122-403.

23. Theoharis, *Chasing Spies*, pp. 114–141.

24. Ibid., pp. 36–41, 114–31.

25. Ibid., pp. 48–49, 84–93; Theoharis, *Spying on Americans*, pp. 100–105.

26. Nigel West, *The Illegals: The Double Lives of the Cold War's Most Secret Agents* (London: Hodder and Stoughton, 1999), pp. 116–26; Robert Lamphere and Tom Shachtman, *The FBI-KGB War: A Special Agent's Story* (New York: Random House, 1986), pp. 273–77.

27. John Barron, *Breaking the Ring* (Boston: Houghton Mifflin, 1987), pp. 3–22, 40–137.

28. Tim Weiner, David Johnston, and Neil Lewis, *Betrayal: The Story of Aldrich Ames, an American Spy* (New York: Random House, 1995), pp. 3–9, 13–17, 32–43, 81–99, 110–20, 128–66, 190–95, 200–52, 276–91; Mark Riebling, *Wedge: The Secret War between the FBI and CIA* (New York: Knopf, 1994), pp. 413–15, 430–33, 441–47.

29. David Wise, *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America* (New York: Random House, 2002), pp. 3–4, 7–8, 18–22, 24–27, 37–42, 50–68, 74–84, 94–99, 107–8, 117–19, 122–42, 159–60, 162–247.

30. Other known cases include Erich Gimpel, William Colepaugh, Gaik Ovakimian, Andre Shevchenko, William Remington, Kaarlo Tuomi, Ann and Robert Baltch, Ivan and Alexandra Egorov, Morris and Lona Cohen, James Harper, Daniel Richardson, Allen Davies, Jonathan Pollard, Edward Howard, Ronald Pelton, Wen Ho Lee, Richard Miller, Thomas Kavanaugh, Larry Wu-Tai Chin, David Barnett, Karl Koecher, Sharon Screnage, Nelson Drummond, Joseph Garfield Brown, Valery Markelov, William Whalen, Herbert Boekinhaupt, Felix Bloch, Earl Pitts, Harold Nicholson, Stanislau Gusev, Katrina Leung, Brian Regan, Ana Montes, Gennadi Zakharov, Christopher Boyce, Marian Zacharski, and Stephan Lipka.

31. *New York Times*, September 17, 2005, p. A1.

32. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: Norton, 2004), pp. 225–27, 239, 258, 261–62, 272; U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, *Report on Joint Inquiry into the Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 107th Cong., 2d sess. (2003), pp. 20–22, 325–35, Appendix: The Phoenix Electronic Communication (redacted text of Williams's July 10, 2001, report to FBI headquarters); *New York Times*, May 4, 2002, p. A10; May 9, 2002, p. A22; June 19, 2002, p. A18; September 25, 2002, p. A12.

33. For examples of such uses, see Theoharis, *Chasing Spies*, pp. 139–234 and Theoharis, *Spying on Americans*, pp. 133–95.

5

THE IDEA OF A EUROPEAN FBI

RHODRI JEFFREYS-JONES

THE IDEA THAT THE EUROPEAN UNION (EU) should create its own equivalent of the U.S. Federal Bureau of Information (FBI) has been in circulation for some years. Clearly, 21st-century terrorist attacks, such as those on September 11, 2001, the Madrid bombings of March 11, 2004, and the London bombings of July 7, 2005, have added zest to discussions of the issue. Attention has focused largely, if not exclusively, on the European Police Office, an EU agency founded in 1999, headquartered in The Hague, and universally known as Europol.

Although the phrase "European FBI" trips off tongues and keyboards with some frequency, the position is anomalous. Commentators are sometimes erudite on Europol and its history, but they have shown little knowledge of the FBI itself and of its suitability (or lack thereof) as a model for Europol. Officials in Europol or involved in its governance characteristically deny that any emulation is taking place. German Chancellor Helmut Kohl, a keen promoter of European police cooperation, apologized in 1997 for using the phrase "European FBI." Europol official Søren Kragh Pedersen noted in 2005 that there was no talk of the FBI at Europol headquarters, even if he hinted at some ambivalence because the FBI was "still a good brand name." Yves Joannesse, Europol desk officer at the European Commission, observed in the same year that some commentators were ignorant of Europol and designated the agency a European FBI only in a lazy act of "copy and paste."[1]

There are, then, several reasons for inquiring into the idea of a European FBI. One is simply a matter of originality: Such research has not previously been conducted in a rigorous fashion. Another is the need to explore the contradictions between popular rhetoric about a European FBI and the realities of Europol and the FBI, respectively. If misperceptions have occurred, the historian must dissect

them and suggest the reasons they arose. Still another reason for the inquiry might be curiosity about the processes by which ideas are, in general, transmitted across the Atlantic. Finally, and more assiduously pursued in this chapter, there is the less arcane issue of what the Americans would call "public history," that is, the utilization of history for public betterment and improved government. In other words, on the evidence of contemporary history, what lessons for Europol-led police cooperation can be adduced from studying the history of the FBI?

On the face of it, Europol is a small organization with less than one-twentieth of the personnel of the FBI and a larger population base to serve, so the comparison may seem strained. However, this essay does posit a number of lessons to be learned from the American experience (as well as some areas in which the FBI could learn from Europol). The history of the FBI over a century or more suggests a need for an expanded Europol with at least some federal laws to uphold, for parliamentary oversight, for ethnic and racial diversity, for commitment to the promotion of the Charter of Fundamental Rights of the EU, for proactive analysis to supplement responsiveness to member state police forces in the field of intelligence collection and analysis, and for liaison with member states' intelligence services in anticipation of the development of that would-be phenomenon, a European foreign intelligence service.

The sources for this chapter, as one might expect, are a blend of printed and digital sources on one hand and, on the other hand, primary sources such as unpublished documents detailing the deliberations of Europol's governing body, the EU's Council of Ministers, and, given Europol's recent provenance, oral history interviews. To round out this preamble with a methodological observation, it seems appropriate to note that one is comparing slow and fast history: The United States is much older than the European Union, and the FBI evolved over a substantially longer period than Europol. If Europol has become an incipient FBI, it will have been as the result of accelerated history.

It remains to examine, in turn, various dimensions of the problem of Europol considered as a European FBI. The administrative history of Europol will not be dealt with here because it has been adequately traced elsewhere.[2] The politics of Europol in individual member states and the way in which the FBI issue has played out in those nations is rich and intriguing (in the United Kingdom, for example, there have been calls for a "British FBI"),[3] but such matters are left to future students of history and government. Here, attention will be given successively to the historical background to the international transmission of police intelligence lessons, impediments to understanding, the reception of foreign ideas, the anatomy of European perceptions of the FBI, enumerated facets of actual FBI history and practice of possible relevance to EU/Europol history and development, and, in conclusion, lessons and cautions suggested by the American experience.

To say that American ideas may have migrated to Europe is hardly revolutionary. From Copernicus to Karl Marx, the intra-European transmission of thought has been a self-evident fact, and European ideas have also traveled

further afield. They have beaten a path to America, which, in being well trodden, has furnished a means for reverse intellectual migration. Just as the American founding fathers were recognizably creatures of the European Enlightenment, so the European Union, though largely a response to war and the product of local leadership, came about partly as the result of American encouragement of the idea of a "United States of Europe."[4]

European experiences of policing and intelligence inspired study and occasionally emulation in the United States. The FBI's precursor, the Bureau of Investigation, was established informally in 1908 and given its name the following year. It was also in 1909 that the British domestic security service, MI5, came into existence, but unaware of that, Congress looked to France and protested that the methods of Napoleon's police chief Fouché were being introduced to their country. Soon thereafter, the administration of President William Taft established a Commission on Industrial Relations that looked abroad for inspiration on how to police class violence, and its Research Division concluded that Germany provided the best model.

In the 1930s, FBI Director J. Edgar Hoover wanted to emulate Scotland Yard. According to one school of thought, the British model was the inspiration for the Office of Strategic Services (OSS, established in 1942) and its successor, the Central Intelligence Agency (CIA, established in 1947). In response to the 1960s race riots, a national commission sponsored work on international comparisons. Soon afterward, Princeton University initiated a study of the FBI that elicited comparisons with the Criminal Investigation Departments of British police forces. In the aftermath of September 11, 2001, there was a powerful agitation in the United States, still unsuccessful at the time of this writing, for the FBI to be scrapped in favor of an American equivalent of MI5 (principally on the ground that MI5 concentrates on intelligence work without the distraction of law enforcement duties). Meanwhile, Harvard University supported a study by Adrian Fortescue, formerly Director General for Justice and Home Affairs at the European Commission, on the new U.S. Department of Homeland Security, in which the author suggested that the "EU might learn, but also perhaps teach." Although Americans are prone to think of themselves as isolationist and anti-intellectual, they have been by no means incurious about intelligence and police practices in Europe.[5]

All this suggests a two-way highway. But the idea of a European FBI has provoked opposition. The citizens of member states have periodically suffered from bouts of xenophobia making them liable to oppose *any* foreign idea. Playing the role of big fish in little ponds, their leaders were prone to fight for the preservation of national sovereignty. Member state leaders like Chancellor Kohl had to curb their enthusiasm for European cooperation in police matters not just to appease their own citizens but also to preserve good diplomatic relations with their peers in other countries. They had to remember that it was only in 1991 that the Maastricht Treaty extended the EU's competences to create a legal basis for cooperation on justice and home affairs that included policy cooperation.

The cultural threat posed by the United States could raise hackles in non-Anglophone areas of Europe. The EU allocated funds to the preservation of minority languages like the author's own, Welsh, but there remained the problem of which language or languages should be used for official EU business. When the EU's Council of Ministers debated the first Europol convention, the working papers and minutes were mainly in English. The French lodged several objections. It is easy to see how people might unconsciously recoil from a policing solution that was pre-packaged in the English tongue and seemed to be modeled on solutions in a far-off English-speaking country.[6]

The issue of national sovereignty has been important in the debate. Not recognizing the analogy with state sovereignty in the United States, European federalists have tended to develop the view that the EU model for cooperation is unique, and perhaps instructive for the North American Free Trade Association (NAFTA) and other such entities. The European equivalent of what Americans call "exceptionalism" militates against receptiveness to the idea of a European FBI.

Other factors conspiring against the idea of a European FBI have been resentment of American power, and the unpopularity of the George W. Bush administration especially because of the Iraq war. Additionally, there is the problem of what one German scholar called the "not always glorious history" of Europol, which has had financial scandals. Perhaps even more damaging to the prospects of emulation were high-profile criticisms of the civil rights record of the FBI, and the concerted post-9/11 criticism of the FBI within the United States on the grounds that more than any other agency it had been responsible for failures in prediction and preemption in the months preceding the attacks on the Twin Towers.[7]

A profile of European perceptions of the FBI-Europol issue might appropriately start, then, with the denials of any link between the two agencies. One tendency has been denial by omission. For example, Europol Director Max-Peter Ratzel, in addressing the European chapter of the FBI National Academy in September 2005, circumspectly embraced the FBI as a partner, rather than as a model. Other denials have been more blunt. Willy Bruggeman, deputy director of Europol, stated in 2000, "Europol is *not* an FBI and is not intended to become a comparable instrument of the EU." In 2002, the sentiment found its way onto the frequently asked question section of the Europol website: "Is Europol a European FBI? No." Singly, it would be possible to take such statements at face value. Their frequent and emphatic repetition, however, brings to mind the words of the Danish prince: "The lady doth protest too much, methinks."[8]

That would certainly be the view of those who have opposed Europol outright on the grounds that it uses FBI practices that will lead Europe down the road to a police state. Prominent in this camp has been the British civil liberties group Statewatch. In 1995, Statewatch's Tom Bunyan greeted the adoption of the Europol convention with a pamphlet arguing that the new organization was the result of a 1980s conspiracy by British, German, and other police chiefs to

promote "the idea of a European-style FBI." The convention had been "drawn up in secret," the European Parliament had not been consulted, and there was no provision for parliamentary oversight. By the time Statewatch's Ben Hayes wrote an additional pamphlet on the issue in 2002, Europol was installed in its offices in The Hague and had started work. The line of attack remained the same, Hayes's tract being subtitled "towards an unaccountable 'FBI' in Europe" and a section in the Statewatch website was titled "EU-FBI surveillance plan."[9]

According to Niels Bracke, a senior official at the General Secretariat of the EU's Council of Ministers charged with Europol and antiterrorist liaison, Bunyan and his colleagues grossly overestimated the powers of Europol and saw abuses where none existed. But Statewatch's critique won a sympathetic hearing in at least one conservative quarter, *The Daily Telegraph* (as this reminds us, conservatives have a claim to the libertarian tradition). Commenting on Statewatch in the wake of a 45.9 percent boost in Europol's budget post-9/11, a Brussels correspondent wrote that Europol seemed to be developing into "a sort of joint FBI/CIA wrapped together in The Hague." It was further acquiring the kind of powers that had "allowed the FBI in Washington to gain the whip-hand over the U.S. state and city police forces." Members of the British contingent in Brussels worried that any hint of an aggregation in Europol powers would provoke stories in the populist press about the return of "jackboot" (fascist) practices in Europe.[10]

The penultimate observation suggests an equivalence between the states' rights issue in America and the national sovereignty issue in Europe. Member states were wary of police integration. For example, in spite of strong support from the British police for the creation of Europol, in 1995 the Home Office shrank from the prospect of operational cooperation. In the words of its spokesman, Peter Wrench, "the original proposal for Europol envisages a sort of European FBI and that idea has not gone away on the part of some countries, but a clear majority are against going in that direction in the foreseeable future." A House of Lords report warned of the need to be on guard against "great dangers to individuals."[11]

As in the case of the United States, one might argue, a plea for citizens' rights could be a fig leaf for assertions of states' rights/national sovereignty. The United Kingdom, ever the South Carolina of European politics, decided not to sign the additional Europol Protocol of 1996, whereby the European Court of Justice could rule on interpretations of the Europol Convention. The election of a new Labour government in 1997 seemed to promise more openness to European cooperation, with Foreign Secretary Robin Cook endorsing police cooperation at European level. But in 2003 the House of Lords (the forum for Britain's senior judges) issued a further report that was critical of the 2002 Europol/United States agreement facilitating the exchange of personal data, complaining that "the draft agreement was deposited very late, when it appeared that the text had already been agreed with the United States."[12]

Other objections to the idea of Europol becoming a European FBI hinged on the matter of constitutional impracticality, with a perception of the problem

having been compounded in 2005 by the failure of France and The Netherlands to ratify the new European Constitution.[13] The proposed constitution would have created European laws, ironed out local constitutional difficulties over the recently introduced European arrest warrant, increased parliamentary oversight, and improved police cooperation. Its defeat perpetuated what one academic study called a state of "legal limbo."[14] Early in 2006, the Austrian presidency emphasized the need to upgrade Europol as well as the general constitutional "architecture" of EU internal security.[15] But for a while, at least, the prospects for a more expansive role for Europol had looked bleak.

Fear of the unknown can be another factor, and here ignorance of the FBI plays a role. The dearth of studies that actually take account of the FBI's history in assessing its modularity for Europe is conspicuous. True, the field is not entirely barren. American political scientist John D. Occhipinti considered U.S.–Canadian police cooperation as a possible model; but what merits attention, surely, is not whether Canadian policemen can operate in the United States but the system whereby a policeman from Maine cannot arrest a suspect in New Mexico, whereas the FBI in a significant number of circumstances can. Another study, by Leuven-based law professor Frank Verbruggen, offered a valuable analysis of FBI–Drug Enforcement Agency (DEA) relations as a possible object lesson for Europol. However, neither scholar addressed the comparative history of police/intelligence federalism. In the absence of knowledge, copy and paste politics was too tempting.[16]

A further dimension of the profile of European perceptions of the FBI-Europol issue is, at least potentially, the paternity debate. After the Bay of Pigs debacle, President John F. Kennedy famously remarked "victory has a hundred fathers, and defeat is an orphan."[17] On the same principle, the stirrings of a debate over the paternity of an organization are one indication of that organization's rising prestige. There have been acute, even bitter disagreements over the origins of the CIA, and historians are beginning to think anew about the issue of whether the FBI originated in the presidency of Franklin D. Roosevelt, Theodore Roosevelt, or even Ulysses S. Grant. Just so, there are signs of dissent over the provenance of Europol.

Denials are legion of the assertion that the FBI fathered Europol. Malcolm Anderson, a pioneer of research into European police cooperation and Europol, reacted thus to the suggestion that following post-Hoover reforms in the previous decade, the FBI might have become an inspiring model for Europe by the 1980s: "It was Chancellor Kohl who launched the idea of a European FBI in the 1980s. It had nothing to with FBI reforms and was always used as a very vague label, given the very different circumstances of Europe and the USA."[18]

Kohl's role and the wider notion of German paternity have rightly attracted serious attention. Asserting "the Germans have always been the principal advocates of a reorganization of the police in the European Union," Verbruggen suggested some reasons. Germany's location at the heart of Europe bordering nine different countries together with its substantial immigrant population made

it vulnerable to international crime and keen on international policing. As a federal nation with its own federal police agency, the Bundeskriminalamt, Germany thought it could offer its own system as a model. It pressed its case with some urgency because it regarded adequate federal policing as a *safeguard* against any return to a Nazi past—an analysis that put it poles apart from the Statewatch argument that Europol would be a *threat* to liberties.[19]

But even before the Europol convention had been signed in July 1995, the paternity debate had broadened. According to a 1993 study by French security expert Jean-Claude Monet, the ancient Athenians invented modern policing. Systematic French policing goes back to the 13th century, and, in the 18th century, the French system was under discussion as a model for Europe. The French inspired the conference in 1914 that gave rise to Interpol. That organization is still headquartered in a French city, Lyon (in the 1980s, the U.S. Secret Service mounted the first serious challenge to French dominance of Interpol, perhaps one reason for the growth of French support for an American-proof Europol).[20]

Monet asserted that enthusiasm for European police cooperation was never so strong as when politicians were exploiting mass hysteria. Examples of the latter included the advocacy of border controls to curtail international crime, with populists pressing the panic button when Schengen loosened border restrictions—a process that they claimed gave the green light to international criminals. What made nonsense of their rhetoric, Monet continued, was the fact that international crime had already been rampant before the EU reduced its internal barriers. Colorful language about crime waves and gangster syndicates was just one of Monet's bêtes noirs. Among the other inappropriate justifications of police integration that he cited were the "fifth column" rhetoric associated with the German police and the anticommunism of the French intelligence services. Monet actually favored European police cooperation but did not want it to come about for the wrong reasons. For him, although the federal German and American models were significant, the origins of cooperative policing in Europe were multinational.[21]

An example of outright advocacy serves to round out this profile of European perceptions of the FBI-Europol issue. In 2004, member of the European Parliament (MEP) Bill Newton Dunn issued a pamphlet, bearing the insignia of the United Kingdom Liberal Democrats but conveying his personal views, called *Europe Needs an FBI*. Newton Dunn had left the Conservative Party to join the Liberal Democrats because of the Tories' anti-European stance, and, with his political ambitions and even survival in question, felt he was free to an unusual degree to speak his mind.[22]

Newton Dunn had watched the American scene. He both knew and exchanged views with Bob Heibel, a former FBI deputy chief of counterterrorism who, since his retirement, had taught at Mercyhurst College (Erie, Pennsylvania), an institution that helped train intelligence analysts. Newton Dunn's pamphlet did not deal with the FBI extensively, but it did show an awareness of the Bureau's weaknesses, such as its fraught relations with the CIA, and of its

tradition, such as leaving much of America's law enforcement to the local police. This last circumstance showed, Newton Dunn said reassuringly, that a European FBI would not "interfere in national policing."[23]

As his willingness to criticize reveals, Newton Dunn was no FBI dogmatist. Indeed, one development he urged was the creation of a European criminal assets bureau aimed at the confiscation of ill-gotten gains, an approach that the Irish government had pioneered. Much of his pamphlet was a litany of problems that needed to be tackled urgently, including cyber crime, trafficking in heroin and people, gangs, money laundering, car theft, currency forgery, and identity theft. In all these areas as well as in the realm of terrorism, criminals posing a threat to EU citizens were organized internationally, both within and outside Europe. European intelligence and policing could only succeed if organized on the federal principle. As this overview indicates, when Newton Dunn wrote of the FBI, he was using the term to describe both a specific phenomenon that might in some respects be emulated and a general need.[24]

Now I will discuss certain enumerated facets of actual FBI history and practice of possible relevance to EU/Europol history and development. In the manner of what the Americans would call the "public historian," the search will be utilitarian, a reflective exercise in the uses of history.[25] There are pitfalls here. In certain cases, lessons apparently transmitted or transmittable from America are not American at all, having been exported from Europe in the first place. In other cases, similar solutions may have arisen spontaneously and separately on each side of the Atlantic simply because the problems were similar, as was the cultural context within which problem solving took place. Nevertheless, while having due regard for such perils, it is possible to consider selected facets of FBI history, identify European equivalents offering appropriate comparisons, and identify lessons that have been or might be learned.

The constitutional and legal facets of FBI history are of special interest. In 2001 there were, according to one estimate, more than 3,300 federal crimes on the American statute books, with more in the offing as members of Congress saw political advantage in promoting "get tough" legislation.[26] Such a body of legislation gave the Bureau the legal basis for lots of work. It was, however, an outcome that had taken decades of effort and had come about not as a result of the founding fathers' plans, but *in spite of* their constitutional provision. After a period of loose confederation in the 1780s, the United States had adopted the Federalists' plan for a stronger Constitution. This contained at least a partial basis for the exercise of federal police powers. The federal government was charged with national defense, the preservation of the republican form of government in the several states, the protection of U.S. coinage, the administration of higher courts, and (Article 1, section 8) the regulation of commerce "among the several states." But in the compromise that allowed ratification of the Constitution, ten amendments were added, the American Bill of Rights. Here we have a potential complication in interpretation, because the U.S. Bill of Rights was partly based on the Magna Carta and the 1688 English Bill of Rights. However, the last of the

amendments was, in the analysis of law professor Bernard Schwartz, American in origin.[27] And it did have a particular resonance for any federal polity. It "reserved to the States respectively, or to the people," those powers not assigned to the federal government by the Constitution.

For the first seventy years of the new republic, one antifederalist crisis followed another, with both New England and South Carolina threatening to secede from the Union, and the (federal) Bank of the United States being dissolved in 1836. But when the Confederate States did secede in 1861, the Union Army settled the matter by force. With the Union sealed in blood, President Abraham Lincoln's last Cabinet meeting in 1865 authorized the creation of the U.S. Secret Service. In the aftermath of the war, its agents—America's first nationally organized federal police force—operated against counterfeiters of the new "greenback" federal currency, with clear-cut constitutional authority. In the 1870s, on loan as special agents to the Department of Justice (newly formed in 1870), they penetrated the Ku Klux Klan, contributing to its demise (this is the origin of the term "special agent" to designate an FBI detective).

President Theodore Roosevelt decided to create a new Bureau of Investigation within the Justice Department instead of having recourse to the continuous borrowing of special agents. But the corpus of laws for the new Bureau of Investigation to enforce expanded slowly. The 1911 Mann Act (also known as the White Slavery Act) empowered it to operate against those who operated the vice trade across state lines, the interstate commerce clause of the Constitution here coming into its own. In World War I, it displaced the Secret Service as the nation's chief counterespionage agency, a function that it performed again in World War II, the Cold War, and at least until the advent of the Department of Homeland Security, in the recent war against terror. The Bureau's repertoire expanded in other respects, too, at least in the case of interstate crimes. By the 1920s, it was investigating automobile thefts. By the 1930s, it was hunting down kidnappers.

There was still no federal crime of murder. "Jumping the fence" became a standard ruse for gangsters on the run—they would reach the state line (or even just the county line) and the cops in hot pursuit would skid to a halt, with the FBI unauthorized to offer help except by circuitous means. Al Capone went to prison for tax evasion, not homicide. The National Association for the Advancement of Colored People's (NAACP) interwar campaign for a federal antilynching law seems irrational (why make murder a double offense?) until one realizes that Southern states were not enforcing their murder laws when the victims were black. But the NAACP failed in its effort to create a special federal crime of murder. In the case of many other serious crimes, too, FBI special agents simply advised on the basis of their specialist expertise or assisted at the scene under local supervision.

Here, however, it is appropriate to take note of a view expressed in 1950 by Edward S. Corwin, a Princeton University professor emeritus who had served in the Department of Justice and was America's leading authority on the

Constitution. He argued that the emergencies of the Depression and World War II had boosted the powers of federal government not just directly but also as the result of the provision of federal assistance in local cases. In positing that in recent cases the Supreme Court had "definitely discarded" the "enumerated powers" doctrine behind the Tenth Amendment he was, perhaps, overly sanguine.[28] Furthermore, following the exposure of an array of abuses of power by the FBI, both Congress and Attorney General Edward Levi took steps in the 1970s to rein it in. But first President Ronald Reagan and then post-9/11 reformers removed many of the restrictions. In summary, few can doubt that the FBI's powers expanded as a result of the imperatives of modern federal government.

Whereas the FBI acquired the duty of enforcing many federal laws, Europol has had not a single such law to enforce, because there is no such thing as a European statutory crime. In the original debate over Europol's remit, the Greek presidency proposed that the new federal police agency would fight drug trafficking and other serious international crime only where such activities occurred "within the territories of at least two Member States," a provision that remains embedded in the Europol convention. There is a parallel with the U.S. interstate commerce provision here, but the Greek presidency proposal went further. Europol would function only in cases where "the form of crime is liable to prosecution in *all* Member States."[29]

These principles were to endure. Noting that the European Union remained "almost always one step behind" in combating organized crime, the Council in 1997 adopted an action plan with the goal of "harmonization of laws" in the member states.[30] When a new European constitution was under discussion in 2005, it was envisaged that a European Public Prosecutor's Office would have powers to deal with "serious crime having a cross-border dimension," but only after unanimous authorization by the EU Council of Ministers and after obtaining the consent of the European Parliament. The British opposed even this measure, and the reverses in the French and Dutch referenda brought the whole constitutional project to a halt. According to Europol's Pedersen, after the constitutional setback, harmonization of member state laws had to remain the goal.[31]

To make the American analogy, it was as if the FBI could operate only with the passage of uniform legislation in every state in the Union. It might be added that unanimous governance through the EU's Council of Ministers resembles the hypothetical situation whereby American law enforcement would be run by a gubernatorial conference with every governor having to agree to each activity. Little wonder that when further protocols were drafted expanding Europol's functions in minor ways, ratification by member states was spotty. A protocol adopted by the Council of Ministers in November 2003 was to be "adopted by the Member States in accordance with their respective requirements," and they were to remember to notify the Secretary-General of the EU if and when they did so. With member states picking and choosing which protocols they wanted to observe, MEP Newton Dunn complained it was difficult to establish who had ratified what. In the aftermath of the 2005 constitutional setback, he predicted that a core of

proactive member states would have to drive through police and intelligence cooperation, leaving the rest to join them later.[32]

On the constitutional front, the lessons of the American model might be separated from the lessons of American history, which are far from reassuring. It took a civil war to cement Lincoln's ideal of an "indissoluble union," and, lest that be considered a pessimistic reflection, let it be remembered that many Southerners still refer to the 1861–65 conflict not as the Civil War but as the war between the states. Hopefully, "member" states will not need that kind of transition. For those who believe that there must be an international solution to international crime and terrorism, the hope must be that European history will be both accelerated and peaceful. Perhaps some reassurance may be gleaned from an apparition of individuals wearing cagoules. These are marked "Europol," and their bearers now hover on the fringes of certain crime scenes and offer expert advice, for example, on the chemistry and likely provenance of new, synthetic narcotics.[33] As Corwin observed, the provision of local assistance can be a first step to greater federalization.

In 1954, J. Edgar Hoover concluded an article with the observation, "Local responsibility, recognized by our forefathers, remains the key to sound law enforcement."[34] Although this is testimony to the FBI director's recognition of the political need to continue to propitiate local sentiment, it belied significant developments over many decades in the powers and functions of American law enforcement. The Judiciary Act of 1789 had created the office of the attorney general, and President George Washington at that time appointed thirteen U.S. marshals, the first federal law officers. In 1870, the attorney general took responsibility for the newly formed Department of Justice, and, in enforcing law obedience in the turbulent South, had the support of U.S. marshals, U.S. district attorneys, and the U.S. Army, as well as the special agents on loan from Treasury. As the number of federal crimes increased, so did the powers of federal law enforcers—by the mid-1930s, special agents were able to make some types of arrest without requesting the presence of local sheriffs and, as all but the most sheltered will know, carried guns and used them.

The EU has no equivalent of federal marshals, federal attorneys, or a federal police force, and Europol staff can neither make arrests nor carry guns. According to Niels Bracke, there is no perception of any need for such practices, as the police forces of the EU member states are stronger and better organized than their equivalents in the states of the American Union. This is a topic that invites further research.[35]

One of the main features of U.S. intelligence history is boosterism. Ambitious agency leaders have been publicists. They converted America's woes into institutional blessings. Major augmentations in federal expenditure and responsibility followed in the wake of crises. It happened not just in the Civil War but in all subsequent wars, too. If no war was at hand, another crisis would suffice: the prostitution scare of 1911, the Red Scares of 1919 and the 1950s, the gangster scare of the 1920s/1930s, 1960s radicalism, crime waves, Chinese espionage

in the 1990s, and Al Qaeda, the latest "threat du jour" as one U.S. intelligence veteran put it.[36] Money was sometimes poured into the solution of problems that had already passed or had been simply invented by some canny booster.

None was better at publicity than the FBI's long-time director, J. Edgar Hoover. But by way of qualification, even Hoover failed, in spite of his many real achievements and in spite of his exceptional gift for public relations, to become a national intelligence czar. That notion has been debated since the 1940s, yet has triumphed only recently, when both the congressional and the independent inquiry into 9/11 recommended the idea.[37]

There have been some glimmerings of such facets of the FBI's past in the relatively brief history of Europol. Newton Dunn recalled the strategic assessment of Jürgen Storbeck, Europol's director until 2004. Storbeck believed that Europol would achieve take-off only after some great crisis, perhaps a financial scam that threatened the stability of European banking.[38]

The prospects for such a shock may be quite real, not least psychologically. As Monet observed, red scares and apocryphal crime waves are no strangers to European history. MEP Claude Moraes, like Newton Dunn an active member of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, observed that police politics is "fashion driven." After the Madrid bombings, European Commission President Romano Prodi promised to increase EU spending on security research to 1 billion annually by 2007, matching the spending of the U.S. Department of Homeland Security. On July 12, 2005, in the wake of the London bombings, the EU's Justice and Home Affairs Council met in emergency session. Within two months came the announcement that, in August alone, €15 million had been pumped into security-related research. A cynic might be moved to observe that over twelve months, that would yield just €180 million, far short of the €1 billion mentioned by Prodi. Even the €15 million was contingent on budget agreement by the member states, which turned out to be a contentious issue under the British presidency the following year.[39]

European leaders, then, may be susceptible to gesture politics. But Europol is not. Storbeck, an unassuming man who reminded Newton Dunn of the U.S. television detective Columbo, was not the kind of person to "invent" a crisis where none existed. Even if Storbeck had wanted to issue sensational press releases, he would have been deterred from doing so. When the Europol convention was under discussion in 1994, the German delegation urged that "press briefings or any other form of public communication on matters concerning Europol . . . shall not be engaged in without . . . the consent of the relevant Member State authorities." Ten years later, Europol still took care to inform and consult member state police forces before issuing press releases on sensitive issues.[40]

Europol is not entirely unconscious of its image. It has responded to approaches from the film industry. In 2003, *Den Tredje Vågen* (The Third Wave), a thriller directed by Anders Nilssen and based on Europol, was the most expensive Swedish movie ever made. Its $4.5 million budget did not, however, match Hollywood extravaganzas. In 2004, *Ocean's Twelve* was a Hollywood thriller

with a Europol dimension and featured a top-notch cast—Welsh actress Catherine Zeta Jones, together with Brad Pitt and George Clooney. Zeta Jones obligingly allowed herself to be photographed clad in a Europol T-shirt, and the portrait thereafter lifted the gloom in the corridors of Europol HQ. But *Ocean's Twelve* was a sequel movie made just to exploit the success of *Ocean's Eleven* and did not really succeed. Zeta Jones refused to allow her photograph to be used for publicity purposes. Staff at Europol HQ shook their heads and said real agents weren't like that, anyway. There was simply no comparison with the promotional impulse behind the G-men films Hoover encouraged in the 1930s, a genre that prompted a whole industry of FBI movies and even mutated, in a case of celluloid exceeding reality, into "The Postmodern G-Man," and "The New Age G-Man."[41]

Charismatic though Hollywood may be, the promotional lessons learned from America seem to have been mixed. Although European politicians can be opportunist, boosterism has not emanated from Europol directly. In 2004, New York–born Gijs De Vries, having served as Dutch deputy interior minister, was appointed to be what the BBC called Europe's new "terror tsar," and he did liaise through Bracke with Europol.[42] But this was hardly an outcome of long-term promotional activity orchestrated from The Hague. The lesson of American history is that overly robust agency promotion leads to distorted spending patterns with the money going to those gifted at publicity, not those who do their jobs well. The hard sell also led to mission distortion with resources being wasted on populist causes.[43] Boosterism is best avoided, and in this area the Americans would seem to have something to learn from Europe, not vice versa.

"Gestapo phobia" has been a further facet of FBI history of possible relevance to EU/Europol history and development. U.S. fear of the Gestapo is just one manifestation of a long trend—in the 20th century, Americans were deeply opposed also to manifestations of Fouché-style or NKVD/KGB-style political policing in their country. But in the immediate wake of Himmler's excesses, there were particular concerns, first that the OSS might become an American Gestapo, and then that the FBI might enact that role. The specter infused new life into American civil libertarianism. Of greater concern here, though, is the political administrative reaction. In spite of a dawning realization that poor intelligence coordination had contributed to America being caught unawares at Pearl Harbor, the Truman administration decided in 1947 to split the intelligence function, with the CIA being given the foreign job and prohibited from operating domestically and the FBI being stripped of its Latin American empire and restricted to domestic counterespionage and police work. The two agencies feuded, fought turf wars, and, in the run-up to 9/11, failed to exchange crucial data.

In Europe, too, there have been civil liberties concerns. Ironically, Statewatch depicted the FBI, at one time the victim of Gestapo-bogeyman politics, as a bogeyman in its own right. Monet complained about the lack of EU transparency in police matters. MEP Sarah Ludford and her civil liberties allies spoke out in 2002 against the dangers of personal data sharing between the Schengen

Information System (an internal EU crime data base) and Europol and between Europol and non-EU countries like Russia and the United States. It is here worth recalling the *Telegraph*'s complaint of Europol's being a "joint FBI/CIA wrapped together." Ludford continued to voice her concerns in 2005 warning about the dangers inherent in the retention of EU border-control personal details. But Ludford's fellow parliamentarian Claude Moraes reflected on the small size of Europol (just 535 staff in all categories in November 2005), which made it much too nonthreatening to be regarded as Gestapo-like. EU external intelligence work has also been relatively modest, with expenditure in 2000 running at approximately one-twentieth of the U.S. level.[44]

In December 2005, the European Parliament, Commission, and Council of Ministers agreed on a deal whereby intercepted telephone calls, text messages, and Internet connections could be retained for between six months and two years. U.K. Home Secretary Charles Clarke, who had been pressing for such a data retention measure, said he was "not so much offended by the use of the words 'police state' or drawing comparisons to Hitler or Stalin, I just regard them as absurd." Interviewees for this project concurred in the view that Europol was a most unlikely reincarnation of the Gestapo. It was partly modeled on modern German police practice, with German policemen prominent in its leadership—and one of the imperatives of postwar German policing had been to stamp out any semblance of Gestapo-like malpractices.

In the view of some of the interviewees, it was testimony to Europol's benign nature that the public had made little use of the EU freedom of information provision in regard to its activities. Also, there had been few complaints since the 1997 Amsterdam Treaty had made it possible for citizens to approach the European Ombudsman about maladministration at Europol. Between 1999 and 2003, for example, there were only eight complaints to the Ombudsman, most them about access to documents and staff issues and mostly upheld, but none of them particularly controversial in character.[45]

Bracke added a further type of rebuttal of the hypothetical Gestapo charge. Deprived, as it is, of arrest powers, Europol has been and remains an investigative, analytical intelligence agency. It does increasingly provide on-the-spot assistance in inquiries but otherwise leaves police operations to the forces in the individual member states.[46]

Europol, in short, is what the post-9/11 FBI is meant to aspire to: a coordinating intelligence agency. That is not to say that it has solved all the problems of analysis. For example, the challenge of recruiting intelligent and qualified analysts is as problematic in Europe as it is in America. The FBI has traditionally been staffed by brave men bearing guns, rather than by thinkers. Hoover wanted to offer measurable proof of the Bureau's efficacy, so he emphasized the need to make arrests and to secure convictions in court. This "arrest culture" often ran contrary to intelligence needs—should one arrest a terrorist suspect or follow him until he leads one to his controller? Post-9/11, the substitution of analysis for "getting a result" has been an uphill struggle.

The CIA, too, has had problems from its earliest days, as the 1950s Doolittle inquiry indicated. Talented members of the military did not want to waste part of their careers serving an agency lacking any power to promote them to a higher grade of general or admiral. Talented scholars shirked employment that would put their publications and academic promotion on hold and leave them tainted with a secret service stigma.[47]

Europol has had similar problems. Staff were seconded from the police forces of the member states, but when they returned to their own countries they found, like CIA agents, that they had marked time in terms of their careers and had to resume at their former ranks—this applied, for example, to Jürgen Storbeck on his return to the German police.[48] There was a danger that talented officers would be deterred from applying for Europol posts, and indeed Director Ratzel made a special plea at the January 2006 Council of Ministers in Vienna for Europol service to be recognized as a criterion for promotion in member state police forces.[49]

However, the fact that Europol has similar recruitment problems to the FBI and CIA does not detract from what many on both sides of the Atlantic would see as a structural superiority—there are no active police duties to contaminate its intelligence work. Though it seems unlikely that the FBI will ever give up its powers of arrest, perhaps here, too, the Americans can learn from Europol.

It is now time to turn to a further facet of FBI history and practice of potential relevance to EU/Europol history and development. The racial dimension of FBI history is notorious. For many years (1924–72), the Bureau was under the leadership of a racial conservative. Shortly after taking over, Hoover dispensed with the services of two of the few African American special agents in the FBI's employ, and thereafter he both resisted the hiring of blacks and persecuted leaders of the civil rights movement such as Martin Luther King Jr. More recently, questions have been asked about the FBI's apparent eagerness to investigate people of color and non-Christian faith and about its failure to recruit Arab American prospective agents in spite of a pressing need for diversity in the fight against terrorism.

But it must be emphasized that there is another side to all this. The first time the Justice Department hired special agents (in 1871), it was with the goal of suppressing Ku Klux Klan terrorism to the benefit of the African American population of the South. Again in the 1920s (and with Hoover playing a leading role), the Bureau moved effectively against the Klan. Between 1940 and 1952, special agents enforced the antilynching program of the Justice Department's new civil rights unit. In the 1960s, with Hoover still in charge, the FBI effectively (indeed ruthlessly) moved against what was a virtual reincarnation of the Klan, the White Hate movement. In making comparisons with Europe, then, both sides of the coin need to be considered.

In 2005, African Americans made up 9.7 percent of the U.S. House of Representatives—a shortfall in that they comprise 13.3 percent of the population. But the FBI was in a different league: blacks (as of 2003) composed just 5.5 percent of its special agent force.[50] Out of a total of 11,500 agents in the FBI in 2003, there were still only about 6 Muslims. The 2000 census listed 1.3 million Arab

Americans officially present in the United States, and the real number may have been three times as high. Yet a mere twenty-one agents were able to speak Arabic.

Europol, like the FBI and CIA, is composed of what one might call "officers" and "other ranks"—security guards, cleaners, secretaries, computer technicians, and so on. The equivalent of the FBI's "special agent" or the CIA's "intelligence officer" in Europol is the bold employee, so called because his or her job description is printed in bold, the requirement being that prior to joining Europol the holder of such a post must already be a policeperson in his or her own country. As of 2005, Europol did retain the nonbold services of multicultural Dutch citizens, a reflection of Netherlands legal requirements (in a visit to Europol headquarters, this researcher spotted two of the several people of color employed, a guard and a secretary). But the bold force was all white, with no Muslims. Following the EU's enlargement to the south and east, Europol was acquiring a capability in the new European languages, but there was much less emphasis on Arabic and Farsi, in spite of the importance of those languages to antiterrorist work.[51]

Europol (and its supporters) defended itself against the charge of prejudice on a number of grounds. Though it could advertise nonbold jobs in the local Dutch press, employees in the bold category were either seconded by the police forces in their own member states (in some cases being paid by their seconding employers) or successful applicants from police backgrounds in member states. Europol had no control over the hiring practices of those member state police forces. The suggestion was that, excepting the British police with its policy of proactive recruitment of minorities, the police forces of Europe were largely prejudiced against minorities, a circumstance that affected Europol's recruitment pool. Another defense, one of the type that is heard in America, too, is that a minority group applicant, for example, a Frenchman of Magreb ancestry, might be less qualified than a white candidate or less trustworthy because he would sympathize with Muslim terrorists. Such persons should not be appointed just because of political correctness.[52]

A further defense was that Europol is no worse than the EU's institutions as a whole, which are generally white and culturally Christian. This is true. I attended a plenary meeting of the Committee on Civil Liberties, Justice and Home Affairs. In an imposing and crowded committee room that would dwarf the entire parliaments of some nations, the back rows on that particular day were occupied by tourist groups from former European colonies, all black. A few rows in front of them sat privileged officials and observers, all white. The inner core consisted of committee members. Although the committee does contain MEPs of color (Claude Moraes and Saj Karim, a Muslim), the inner core, too, was on that day uniformly white. On that particular day, one could have been forgiven for thinking that the Third World had come to learn from its master.[53]

Both because of his concern for racial justice and because he thought jihadism was a real problem, Moraes has devoted thought to these problems and offered some additional reflections. Europol advertised posts, he thought, in places where ethnic minorities never looked. French postcolonial thinking prevailed—like

Spain and Portugal in their New World colonies, France maintained the fiction (even through the race riots of 2005) that every inhabitant of metropolitan France had equal citizenship and opportunity, regardless of ethnic or religious background. According to this mode of thought, actively seeking nonwhite bold appointments would have been illogical and quite unnecessary. For Moraes, the problem was not just a French one. In Eastern Europe with its newly acceded member states, there were ten million Roma (the gypsies that Hitler despised so much), but they were absent from the ranks of the local police and thus Europol. Why was there no agitation on such issues? Europol was a small organization that operated behind the scenes. It was because of this obscurity that its lack of diversity had not become a public symbol and remained less of an issue.[54]

Here is an instance where Europe can learn. Racial tolerance is a just goal in ethical terms. In social terms, it reduces divisiveness, and with it the likelihood of collective unrest, treasonable betrayal, and individual acts of terror. In functional terms, it enables police and intelligence agencies to recruit more widely, giving access both to a larger pool of talent and to people with special skills such as local knowledge or non-European languages and dialects. Post-9/11 investigations in the United States implicitly recognized such factors and recommended greater hiring diversity in the FBI and its sister agencies. The EU might consider a similar course of action.

Students of the drug addiction problem in America will be aware of another facet of FBI history having a potential bearing on Europol: the Two Prohibitions hypothesis. The prohibition of alcohol in the 1920s was then and is still regarded as having been an expensive failure. There are those, whether on the left of the political spectrum or neoconservatives like Milton Friedman, who would argue that the current narcotics prohibition is a mindless repetition of a historical error. Be that as it may, the American war on drugs fueled FBI expansion directly and, as Verbruggen noted, indirectly through the Bureau's absorption of the DEA.[55]

The parallel with Europol is plain, as the European Drugs Unit (established in 1994) preceded it. Other functions such as anticounterfeiting operations stimulated federal police work in Europe as they had in America, but the war against narcotics had a popular appeal that spread far beyond the banking fraternity. The new designer drugs penetrated suburbia and affected the offspring of politically influential middle-class parents. In the 1994 formative debate on Europol, the drug issue went from strength to strength. In March, the Greek presidency proposed that Europol should fight "1. Terrorism. 2. Other forms of crime." By May, the formula was "1. Terrorism. 2. Unlawful drug trafficking. 3. Other serious forms of international crime." Ten years later, Europol's annual report listed its crime priority as "drugs trafficking," followed by five other categories.[56]

Verbruggen saw the politics of drugs policing as playing a key role in the United States and Europe alike, with "Americanization" of European policing taking place and with the "over aggressive" crusade against drugs doing damage to police structures on both continents, even if Europol was "unlikely to become a European FBI." [57] However, another perspective might be that drug politics has

been the engine of police cooperation, perhaps not a desirable phenomenon in itself, but a means to an end. Politicians may never admit that prohibition has been a mistake with a happy outcome, but historians on both sides of the Atlantic are free to speculate in that regard.

This brings us to another facet of the American experience—parliamentary oversight and politics. To legislators' fury, Theodore Roosevelt set up the FBI's precursor during a congressional adjournment. But that was for a special reason—the president's determination to target and root out corruption on Capitol Hill had provoked congressional opposition to his plans. In more normal times, the Bureau has been subject to abundant congressional oversight. Congress has held the purse strings, giving the Appropriations Committees a powerful say, and the heavyweight House and Senate Judiciary Committees, established in 1813 and 1816, respectively, have jurisdiction—the House committee having the FBI specifically in its remit, and the Senate committee being responsible for matters of concern to the Bureau, including espionage, counterfeiting, civil liberties, federal courts, antitrust policy, and revisions of the criminal code.[58] In addition to this, the FBI is subject to the perusal of special investigative committees, such as the Church and Pike inquiries of the 1970s. These in turn inspired new permanent intelligence committees in both houses of Congress that oversaw relevant aspects of the FBI's work.

More than this, the FBI is subject to the scrutiny of the Department of Justice. The attorney general of the United States is appointed by a democratically elected official, the president, and confirmed in office by Congress. Attorneys general have periodically reformed or reshaped the FBI; in their different ways, Charles Bonaparte, Harlan Fiske Stone, Bruce Cummings, Frank Murphy, Edward Levi, and John Ashcroft played roles that could be said to have been of greater strategic significance than those of the Bureau's directors. The Department of Justice also appointed inspectors general to scrutinize particular aspects of FBI performance, and they have sometimes been very critical. For example, in 2002 Inspector General Glenn Fine delivered devastating remarks, based on his audit of the FBI's counterterror performance, to a subcommittee of the Senate Judiciary Committee.[59]

In 1964, journalist Fred Cook published a critical study of the FBI, noting that the Bureau had been "created in secrecy, by executive order, in defiance of the will of Congress." But he added that it had been two "liberal" presidents, Republican Theodore Roosevelt and Democrat Franklin D. Roosevelt, who had created the "all-powerful" FBI.[60] Notwithstanding the fact that recently neoconservatives have made the Bureau their own, the FBI was the outcome of a 20th-century liberalism that, unlike its 19th-century namesake, was statist and thus federalist.

Here, one can detect the glimmerings of a European comparison. Newton Dunn estimated that approximately 90 percent of British Tories opposed the idea of Europol. More liberal parties did not always brim over with enthusiasm, but at least they were not opposed in principle. Looking at the European Parliament, his colleague Claude Moraes estimated that the center-left was broadly in favor of

Europol, especially as it pursued wealthy drug traffickers instead of making petty arrests. The center right, with the exception of the British Tories, was also supportive, but the far right was less keen on police cooperation except on matters like immigration restriction through border controls. Political generalizations and labeling are often unreliable, and it must be conceded that civil libertarian critics of the FBI and Europol are usually liberal/left in orientation, but with those qualifications, it may be said that both the FBI and Europol are the creations of liberal federalists.

But parliamentary oversight is also generally a liberal phenomenon, and this is as conspicuous by its absence from the European scene as by its presence in the United States. The EU's Council of Ministers controls Europol directly and through a management committee. This applies to both Europol's budget and the scope of its activities. The European Commission, which can be seen as a powerful civil service, might be expected to have a strong role, but it is less active than in other realms of EU activity. Europol reports annually to the European Parliament, but on an information-only basis. Europol would like to answer to parliament, and its director has testified before the Committee on Civil Liberties, Justice and Home Affairs on a voluntary basis. The committee is glad to perform this role and would like to expand it. Its members have visited Europol's HQ in The Hague, where they have been welcomed. But in spite of proposals for greater parliamentary oversight, little has happened. Instead, member states have floated the idea that there should be joint oversight by member states' parliaments, as distinct from the federal European Parliament.[61]

In short, by comparison with the United States, the EU has a democratic deficit in regard to the oversight of its federal police. The internal politics of the EU make the Council of Ministers reluctant to allow the Parliament a greater role in oversight of Europol. But the restrictions come at a price. Iron control by the member states may offer a guarantee that Europol will never become an instrument of a European police state, but it cannot offer reassurance to the public of the type that encourages social confidence and willing cooperation with police inquiries. Only parliamentary oversight and investigation can bring that about.

Europol is not a clone of the FBI. There are, however, parallels between the agencies that need to be discussed more fully and candidly. The similarities are sufficient in number to suggest that several lessons might be learned.

In an area like drug policing, neither America nor Europe seems equipped to teach the other. In other areas, in spite of Europol's small size and short history, there already appear to be lessons for America to learn. To this point, Europol boosterism has been kept firmly under control, an achievement that America might profitably emulate in the case of the FBI. If American commentary is to be heeded, Europe would seem to offer another lesson, too. Although it may aspire to a wider role, Europol remains essentially an intelligence agency, something to which the feds—or, at least, their political masters—profess to aspire.

The American Gestapo phobia resulted in an unfortunate domestic/foreign intelligence dichotomy. In the absence of any serious concern about an EU police

state, there is a chance that Europe will be able to avoid this problem—early in 2006, for example, there was talk of an external role for Europol in the West Balkans.[62] Additionally, American mistakes would suggest the lesson that liaison with member state foreign intelligence services and with any EU equivalent that may develop should be a security prerequisite.

In other respects, though, the EU can learn from the FBI experience. While the diversity problem is still serious in America, present-day Europe faces a graver issue. The lack of diversity in policing in both member states and in Europol is an affront to Europe's sizable minority populations and a danger to Europe's whole self. Although Europol's liaison arrangements with member states remain essential, there does seem to be a need for direct hiring at bold level that is monitored according to diversity criteria.

American history offers many instances of the benefits of legislative oversight of intelligence functions, as well as examples of how lapses in oversight can cause things to go wrong. With the Council of Ministers monopolizing oversight, Europe has not yet dared to travel down that road, but should do so. On another didactic front, as the substantial corpus of federal criminal law attests, America has largely overcome the restrictions inherent in its constitutional doctrine of reserved powers. Europe may yet unravel that puzzle. However, a caution is appropriate here. Were the European Parliament to acquire greater powers and legislate in this way, it might give cause for Europol to expand from its intelligence function and become an agency with the power of arrest.

That is a dilemma that merits some thought. At some future point, it may be deemed appropriate for Europol officers to have the power of arrest in special cases, for example, where a local police force is failing in its duty. But there would appear to be a Euro-American convergence of viewpoint on the desirability of an agency that can concentrate on analysis and can cooperate with other intelligence and police agencies without being distracted by turf wars or the need to make frequent arrests to satisfy public opinion.

NOTES

Gwenda Jeffreys-Jones (Coreper Desk Officer, Secretariat General, European Commission) gave advice on this project as well as hospitality in Brussels. Terry F. Cole, a former colleague of the author's at the University of Edinburgh, helped with some German–English translation. EU officials and Members of Parliament, some credited by name in these notes and others anonymously, agreed to give interviews and advice. Staff at the EU Council Library, especially Rita Tuominen and (at the Transparency unit) Lino Liao, could not have been more helpful. A draft of this essay was delivered as a paper to the transatlantic seminar of the School of Social and Political Studies at the University of Edinburgh, where John Peterson and his colleagues offered valuable comments. Further advice came from academic colleagues Malcolm Anderson, Simon Duke, and Charles Raab and from Gustaaf Borchardt, director for Relations with the Council at the

Secretariat General of the European Commission. The United Kingdom's Arts and Humanities Research Council made an award to enable the author to undertake research both for a history of the FBI and for this project. The Leverhulme Trust awarded a Research Fellowship that defrayed the expense of overseas research trips. To all these individuals and institutions, the author is most grateful.

1. Frank Verbruggen, "Euro-Cops? Just Say Maybe. European Lessons from the 1993 Reshuffle of US Drug Enforcement," *European Journal of Crime, Criminal Law and Criminal Justice* 13, no. 2 (1995), p. 152; Jan Ellermann, "Vom Sammler zum Jäger: Europol auf dem Weg zu einem 'europäischen FBI'?" *Zeitschrift für europarechtliche Studien* 5, no. 4 (2002), p. 567; interview with Søren Kragh Pedersen (Public Relations Unit, Corporate Governance and Development, Europol), Europol headquarters, The Hague, November 17, 2005 (hereinafter Pedersen interview); interview with Yves Joannesse (Expert National Detaché, Lutte contre le terrorism, le trafic et l'exploitation des êtres humains, et Cooperation policière, D.G. Justice et Affaires intérieures, Commission européenne), Justice and Home Affairs Building, Brussels, November 22, 2005 (hereinafter Joannesse interview).

2. See, for example, Malcolm Anderson, Monica den Boer, Peter Cullen, William Gilmore, Charles Raab, and Neil Walker, *Policing the European Union* (Oxford: Clarendon Press, 1995) and John D. Occhipinti, *The Politics of EU Police Cooperation: Toward a European FBI?* (Boulder, CO: Lynne Rienner, 2003). Occhipinti's book rarely mentions the FBI and is an administrative rather than a political study, but it provides reliable information both on the formation and development of Europol, and on its EU context.

3. When Home Secretary David Blunkett established the United Kingdom's Serious Organised Crime Agency, it prompted persistent speculation that the goal was a "British FBI": *Gloucestershire Echo*, April 1, 2004; *Independent*, November 24, 2004; *Guardian*, November 14, 2005.

4. See, for example, Thomas C. Fischer and Stephen C. Neff, "Some American Thoughts about European 'Federalism,' " *International and Comparative Law Quarterly* 44, no. 4 (October 1995), pp. 904, 910; John Killick, *The United States and European Reconstruction, 1945–1960* (Edinburgh: Keele University Press, 1997), pp. 9–10.

5. Both in this paragraph and in subsequent passages, a portion of the information is drawn from the author's forthcoming history of the FBI, to be published by Yale University Press. See also Rhodri Jeffreys-Jones, *Violence and Reform in American History* (New York: New Viewpoints, 1978), p. 168; Rhodri Jeffreys-Jones, "The Role of British Intelligence in the Mythologies Underpinning the OSS and Early CIA," in *American-British-Canadian Intelligence Relations 1939–2000,* eds. David Stafford and Jeffreys-Jones (London: Frank Cass, 2000), pp. 5–19; Courteney Ryley Cooper, "Introduction," in J. Edgar Hoover, *Persons in Hiding* (London: J. M. Dent, 1938), pp. vii, ix; Hugh Davis Graham and Ted Robert Gurr, eds., *Violence in America: Historical and Comparative Perspectives, A Report Submitted to the National Commission on the Causes and Prevention of Violence* (New York: Bantam Books, 1969), especially parts I, II, VI, and VII; C. H. Rolph, "The British Analogy," in *Investigating the FBI,* eds. Pat Watters and Stephen Gillers (New York: Ballantine for Princeton University's Committee for Public Justice, 1973), pp. 351–70; Todd Masse, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States* (Washington, DC: Congressional Research Service, 2003); "Intelligence at Home: The FBI, Justice, and Homeland

Security," chapter 10 in *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (March 31, 2005), pp. 466–67; Adrian Fortescue, "The Department of Homeland Security: A Partner but not Necessarily a Model for the European Union," paper given at the Weatherhead Center for International Affairs, Harvard University, July 19, 2004, available at http://www.wcfia.harvard.edu/fellows/papers/2003–04/fortescue.pdf, p. 31. Sir Adrian died shortly after giving his paper, and in his honor the director general of Justice, Freedom and Security issued a new edition of it under the title *A European View of the U.S. Department of Homeland Security*.

6. For examples of French objections to English monoglotism, see General Secretariat (Council of the European Union), "Proceedings of the Europol Group on 29 and 30 March 1994," document 6018/94, Brussels, April 7, 1994, and General Secretariat (Council of the European Union), "Outcome of Proceedings of Europol Working Party," document 6200/94, Brussels, April 12, 1994.

7. Ellermann, "Vom Sammler zum Jäger," p. 584.

8. Max-Peter Ratzel, "Information Sharing—Developing the Framework to Engage Serious and Oganised Crime in the UK and Europe," address to the 23rd annual retraining event of the FBI National Academy Associates European Chapter, Edinburgh, September 27, 2005 (supplied by kind courtesy of Europol); Willy Bruggeman, "Europol—A European FBI in the Making?," lecture under the auspices of the Cicero Foundation, Paris, April 2000, availabe at http://www.cicerofoundation.org/lectures/p4bruggeman.html, p. 11; denial copyrighted in 2002 and still current in January 2006: http://www.europol.eu.int/index.asp?page=faq; William Shakespeare, *Hamlet* (1602–5), Act III, scene ii.

9. Tony Bunyan, *The Europol Convention* (London: Statewatch, 1995), pp. 1, 9; Ben Hayes, *The Activities and Development of Europol—Towards an Unaccountable "FBI" in Europe* (London: Statewatch, 2002); Statewatch website, http://www.state watch.org/eufbi.

10. Interview with Niels Bracke (principal administrator, General Secretariat, EU Council of Ministers), Caledonian Hilton Hotel, Edinburgh, November 28, 2005 (hereinafter Bracke Edinburgh interview); Ambrose Evans-Pritchard in *The Daily Telegraph*, April 27, 2002. On the jackboot fears, interview with Charles Williams (administrator, D-G Justice and Home Affairs, European Commission), Brussels, November 21, 2005 (hereinafter Williams interview), with a similar point being made by Bill Newton Dunn (member of the European Parliament), Brussels, November 22, 2005 (hereinafter Newton Dunn interview).

11. House of Lords, Select Committee on the European Communities, session 1994–95, 10th report, *Europol* (April 25, 1995), pp. 11, 25.

12. *Europol and the EU's Fight against Serious and Organised Crime* (Foreign and Commonwealth Office background brief, May 1997), front cover and p. 2; House of Lords, Select Committee on the European Communities, session 2002–03, 5th report, *Europol's Role in Fighting Crime* (January 28, 2003), p. 16.

13. The author's interviewees talked of constitutional difficulties, and it was Ellermann's concluding observation, "Vom Sammler zum Jäger," 585.

14. Elspeth Guild and Sergio Carrera, "No Constitutional Treaty? Implications for the Area of Freedom, Security and Justice," Centre for European Policy Studies Working Document 231 (October 2005), pp. 3, 5.

15. Press release from the Austrian presidency, January 14, 2006, net. According to BBC News, EU antiterror coordinator Gijs de Vries at this point referred to "a general desire to now see Europol take on an operational role," available at http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/4613508.stm.

16. Occhipinti, *Politics of EU Police Cooperation*, p. 1; Verbruggen, "Euro-Cops?," pp. 150–201.

17. Kennedy quoted in Arthur M. Schlesinger Jr., *A Thousand Days: John F. Kennedy in the White House* (London: André Deutsch, 1965), pp. 262–63.

18. Email, Anderson to author, November 9, 2005. Then professor of politics at the University of Edinburgh, Anderson headed a research project, financed by the United Kingdom Economic and Social Research Council and involving Monica den Boer, Bill Gilmour, Neil Walker, Peter Cullen, and Charles Raab, titled "Policing Europe after 1993." Anderson published widely in the field, the main outcome of the aforementioned project being *Policing the European Union* (Oxford: Clarendon Press, 1995), written in conjunction with his fellow researchers.

19. Verbruggen, "Euro-Cops?," p. 150n3.

20. Jean-Claude Monet, *Polices et Sociétés en Europe* (Paris: La documentation Française, 1993), p. 27; Malcolm Anderson, *The French Police and European Co-operation* (University of Edinburgh: Project Group European Police Co-operation, c. 1992), pp. 3, 5, 28–29.

21. Monet, *Polices et Sociétés en Europe*, pp. 301–5. Those who credit France with an input to proto-Europol thinking point to the work done by President Georges Pompidou (1969–74), who, though a Gaullist, tried to bring his nation out of its nationalist-isolationist shell in police matters. See, for example, Francis R. Monaco, "Europol: The Culmination of the European Union's International Police Cooperation Efforts," *Fordham International Law Journal* 19, no. 1 (October 1995), p. 267.

22. Bill Newton Dunn, *Europe Needs an FBI* (n.p.: Liberal Democrats, 2004. This pamphlet has no pagination, but is divided into enumerated sections and subsections); Newton Dunn interview.

23. Newton Dunn interview; Newton Dunn, *Europe Needs an FBI*, sections 6.2 and 8.6.

24. Newton Dunn, *Europe Needs an FBI*, section 8.3 and passim.

25. Dutch historian Pieter Geyl offered some respected thoughts and warnings in this area in *Use and Abuse of History* (New Haven, CT: Yale University Press, 1955), and, since 1978, the University of California Press has published a journal devoted to its eponymous field, *Public Historian*. Of special interest to readers of this chapter may be David J. Garrow, "FBI Political Harassment and FBI Historiography: Analyzing Informants and Measuring the Effects," *Public Historian* 10 (Fall 1988), pp. 5–18.

26. *Christian Science Monitor*, 25 June 2001.

27. Bernard Schwartz, *The Great Rights of Mankind: A History of the American Bill of Rights* (New York: Oxford University Press, 1977), p. 83.

28. Edward Corwin, "The Passing of Dual Federalism," *Virginia Law Review* 36, no. 1 (February 1950), p. 5.

29. Presidency (Council of the European Union) to Working Party on Europol, "Presidency Proposal Concerning Article 2," document 6016/94, Brussels, March 28, 1994 (emphasis added); *Europol Convention* (Luxembourg: Office for Official Publications of the European Communities, 2004), Title I, Article 2, p. 8.

30. "Action Plan to Combat Organized Crime," adopted on April 28, 1997 (97/C 251/01) in Council of the European Union, *Customs, Police and Judicial Cooperation in the European Union: Selected instruments* (Brussels, 1998), volume A, pp. 5–6.

31. David Phinnemore, "The Treaty Establishing a Constitution for Europe: An Overview," Royal Institute for International Affairs, London, 2004, available at http://www.chathamhouse.org.uk/pdf/research/europe/BN-DPJun04.pdf, p. 17; Pedersen interview. For the text of the constitution proposed in 2003, see http://european-convention.eu.int/docs/Treaty/cv00850.en03.pdf.

32. "Article 2, Protocol amending the Europol Convention adopted by the Council on 27 November 2003," *Official Journal of the European Union* (January 6, 2004), C 2/8; Newton Dunn interview.

33. Pedersen interview.

34. J. Edgar Hoover, "The Basis of Sound Law Enforcement," *Annals of the American Academy of Political and Social Science* 291 (January 1954), p. 45.

35. Telephone interview with Niels Bracke, November 9, 2005 (hereinafter Bracke telephone interview).

36. Arthur S. Hulnick, *Keeping Us Safe: Secret Intelligence and Homeland Security* (Westport, CT: Praeger, 2004), p. 189.

37. *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd sess. (2002), p. 3; *The 9/11 Commission Report* (New York: Norton, 2004), p. 411. For a general exposition of the publicity theme, see Rhodri Jeffreys-Jones, *Cloak and Dollar: A History of American Secret Intelligence*, 2nd ed. (New Haven, CT: Yale University Press, 2003).

38. Newton Dunn interview.

39. Interview with Claude Moraes, Brussels, November 22, 2005 (hereinafter Moraes interview); press release by the Xinhua News Agency, March 17, 2004; Keith Nuttall, "EU Gives £10m Boost to Security Research," *Times Higher Education Supplement*, September 2, 2005; anonymous interview.

40. Newton Dunn interview; German delegation to the ad hoc EU Council Working Group on Europol scheduled to meet on February 17 and 18, 1994, "Germany's Views," document 4776/94, Brussels, February 10, 1994.

41. Interview with Rainer Wenning (Corporate Communications, Europol), Europol headquarters, The Hague, November 17, 2005. For a dissection of the numerous movies made about the FBI, see Richard Gid Powers, "The FBI in American Popular Culture," in Athan G. Theoharis, ed., *The FBI: A Comprehensive Guide* (New York: Checkmark, 2000), pp. 261–307.

42. See http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/3567809.stm.

43. This is the theme of the author's book *Cloak and Dollar*.

44. Monet, *Polices et Societés*, p. 303; Ole R. Valladsen, "Prospects for a European Common Intelligence Policy," *Studies in Intelligence* 9 (Summer 2000), p. 87; Ludford quoted in *European Voice*, October 31–November 6, 2002; author's eyewitness notes on Ludford speech on the Visa Information System in plenary session of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, Brussels, November 23, 2005; Moraes interview; Pedersen interview.

45. Clarke quoted in *European Voice*, December 15–20, 2005; Pedersen interview, Williams interview; "The European Ombudsman Decisions Concerning Europol,"

available at http://www.euro-ombudsman.eu.int/decision/en/europol.htm. The author is grateful to Rosita Agnew of the Ombudsman's office for supplying this information.

46. Bracke telephone interview.

47. "Report on the Covert Activities of the Central Intelligence Agency," Doolittle Report, September 30, 1954, p. 26, in unlabeled box, Modern Military Headquarters Branch, National Archives, Washington, DC.

48. Newton Dunn interview.

49. Anonymous interview; telephone interview with Søren Kragh Pedersen, February 24, 2006.

50. Congressional Research Service, "Black Members of the United States Congress, 1870–2005," August 4, 2005, web, Table 5; 2003 FBI employee statistics for June 30, 2003, accessed June 2004 on FBI website; Table 13, "Resident Population by Sex, Race, and Hispanic Origin Status: 2000 to 2003," U.S. Census Bureau, "Statistical Abstract of the United States 2004–2005," census website (http://www.census.gov).

51. Bracke Edinburgh interview. On American concerns regarding Farsi and other non-European languages, see "Building Capabilities: The Intelligence Community's National Security Requirements for Diversity of Language, Skills, and Ethnic and Cultural Understanding," *Hearing of the Permanent Select Committee on Intelligence*, 108 Cong, 1 sess, 5 Nov 2003.

52. Interviewees who made these points said that they did not personally hold these prejudices, and they wished to remain anonymous.

53. Moraes interview; Newton Dunn interview; author's visit to plenary session of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, Brussels, November 23, 2005.

54. Moraes interview.

55. Milton and Rose Friedman, *Free to Choose* (Harmondsworth: Penguin, 1980), pp. 267–69; Verbruggen, "Euro-Cops?," p. 201.

56. Presidency (Council of the European Union) to Working Party on Europol, "Presidency Proposal Concerning Article 2," document 6016/94, Brussels, March 28, 1994; Presidency (Council of the European Union), Note, "Annex to Article 2 of the Draft Convention on the Establishment of Europol," document 7238/94, Brussels, May 26, 1994; *Europol Annual Report 2004* (The Hague: Europol, 2005), p. 6.

57. Verbruggen, "Euro-Cops?," p. 201.

58. Donald C. Bacon et al., eds., *The Encyclopedia of the United States Congress*, 4 vols. (New York: Simon and Schuster, 1995), vol. 3, pp. 1198–204.

59. Fine testimony to Subcommittee on Technology, Terrorism, and Government Information, October 9, 2002, LexisNexis.

60. Fred J. Cook, *The FBI Nobody Knows* (London: Jonathan Cape, 1965), p. 49.

61. Bracke telephone interview; Pederson interview; Williams interview.

62. EU Council of Ministers President Liese Prokop urged this. Press release from the Austrian presidency, January 14, 2006, net.

6

WASHINGTON POLITICS, INTELLIGENCE, AND THE STRUGGLE AGAINST GLOBAL TERRORISM

GLENN HASTEDT

Politics stops at the water's edge.
All politics is local.

NO GOLDEN RULE HAS YET BEEN FOUND that guarantees success in making American foreign and national security policy. Instead, we find the two competing imperatives presented in the epigraphs. According to the first, "politics stops at the water's edge," foreign and national security policy is made in response to events and forces beyond American borders. The nature of the situation confronting the United States, its internal logic and dynamics, and the actions of other international actors combine to establish the parameters of American foreign and national security policy. There is no room for partisan politics or bureaucratic infighting in shaping this policy. At best they are distracters that lessen the effectiveness of a policy; at worst they doom it to failure by injecting inconsistencies, unwarranted constraints, and contradictions into it. According to the second, "all politics is local," American foreign and national security policy is always made in response to domestic political considerations. It cannot be otherwise. Events beyond America's borders no more demand or dictate a certain policy response than do events inside it. Accordingly, foreign and national security policy does not operate according to a different set of political rules than does domestic policy. Success in each requires accommodating differences of opinion that are rooted as much in self-interest as in points of principle and building winning coalitions that are based on power considerations and not the elegance of an argument.

These two imperatives share an uneasy coexistence. They point in opposite directions, yet each contains elements of truth. Policy makers who fully embrace

the reasoning of one imperative to the neglect of insights offered by the other risk policy failure. Intelligence policy is no exception. Conceptualizing intelligence solely in terms of unmasking conditions and threats beyond American borders so that the proper response can be crafted will not by itself ensure success in the struggle against global terrorism. Intelligence also needs to be understood in the context of the political dynamics that shape the policy process in Washington.

Conventional accounts of intelligence comfortably reside within the confines of the first imperative. Intelligence is discussed as a value-neutral activity whose defining purpose is to help policy makers better understand a situation by furnishing them with analyzed information. The most heated debates have been over whether the intelligence community correctly understands the capabilities and intentions of America's external enemies, whether it be international communism, the Soviet Union, Al Qaeda, or global terrorism. The most frequently employed framework for understanding how such judgments are arrived at is the intelligence cycle.[1] It breaks intelligence down into a series of functionally related steps beginning with setting "needs to know" and ending with the production of intelligence for policy makers.

Less common are accounts of intelligence that build on the second policy-making imperative. Viewed from this perspective, the essence of intelligence is its ability to enhance the political power of those who possess it. The most heated debates here have been over whether intelligence has become politicized. Obtaining an understanding of intelligence's internal dynamics from this second perspective requires a different analytical framework. Rather than see it as composed of a series of functionally related steps that follow one after the other, intelligence can be broken down vertically into a series of different political games or contests that are continuously being played out. Not all of these games are equally visible to the public due to the level of secrecy that surrounds them, nor is the level of activity the same in each game. Some political contests may be relatively quiet and in a state of equilibrium, whereas others may be hotly contested.

In the following sections, four political games that are continuously played out within the intelligence policy area will be introduced. For each I discuss what is being contested and why; I also identify the key political actors. The struggle against global terrorism provides the necessary policy context for the discussion because as the first policy-making imperative correctly notes American foreign and national security policy is designed with an eye toward dealing with a problem. Policy problems and politics cannot be totally separated.

SYMBOLIC POLITICS

Words and images matter in politics. By setting and controlling the language of the political debate and the images that frame it, policy makers are able to provide an inherent advantage to certain policy options over others and favor certain political institutions and actors over others.[2] As such, the words and

images used in policy debates are often contested, but the political contest over symbols is not an even one. By virtue of their ability to command media attention, presidents possess an inherent advantage should they choose to use it. This is especially true in foreign and national security policy, where the president is looked on as the spokesperson for the nation and as the commander in chief. Entering into the arena of symbolic politics is not without risk. Words and images not only serve to control and direct political activity, they also raise expectations and can come to entrap policy makers that employ them.

Post-9/11 intelligence policy in the struggle against global terrorism has been shaped by symbolic politics in at least four different ways. First, it created a political context that favored aggressive collection policies. The George W. Bush administration moved quickly to define the terrorist threat as a war. Employing this imagery was easily understandable and well received by the American public. Both the location of the terrorist attacks of September 11, 2001, and the scale of the death and destruction they brought stunned Americans and produced a deep and palpable desire to reach out and punish those responsible for it. As natural as the war imagery seemed to most Americans, it was not the only way in which to symbolically frame the response to 9/11. Speaking of the British experience with terrorism in Northern Ireland, Michael Howard observed "a struggle against terrorism . . . is unlike a war against drugs or a war against crime in one vital respect. It is fundamentally a battle for hearts and minds. . . . Terrorists can be successfully destroyed only if public opinion, both at home and abroad, supports the authorities in regarding them as criminals rather than as heroes."[3]

From a political perspective, however, the war imagery offered something to the Bush administration that criminal imagery could not. It firmly centered decision-making power and authority on counterterrorism in the White House. It allowed the president to cast himself as a "war president" and in the process, at least for a time, politically disarmed his opponents who, in embracing the war imagery, were obliged to speak in the language of national unity. Just as significantly given the American approach to war, which sharply distinguishes periods of war and peace and favors unilateral action and is loathe to accepting restraints on the use of force, the war imagery allowed and perhaps encouraged the administration to think of intelligence activities in expansive terms. Wars are won or lost and presidents are held electorally accountable. Above all, winning the war on terrorism required preventing another attack on the American homeland, and to this end any and all information on the subject that could be collected needed to be collected.

Second, symbolic politics has been used extensively to reassure the public that the administration was in charge, all is well, and that progress in the war against terrorism was being made in the area of intelligence policy. Just nine days after the 9/11 terrorist attacks, Bush addressed a joint session of Congress and announced the creation of an Office of Homeland Security in the White House. Its director would report directly to the president and be advised by a Homeland Security Council. Tom Ridge, governor of Pennsylvania and a political confidante

of the president was named director. The Office of Homeland Security was to oversee and coordinate the development of a comprehensive national strategy to safeguard the United States against terrorist attacks and take the lead in responding to any that might occur. Positioning Homeland Security and its director in the White House put it out of the reach of Congress both in terms of approving personnel and budget and being able to compel individuals to testify. Such requests, which quickly came, were met with invocations of executive privilege.

Intent on defending its prerogatives, Congress challenged the Bush administration by putting forward legislation to create a Department of Homeland Security whose head would be approved by Congress and whose budget would be authorized by it. In keeping with the war imagery, Congress did not present its plan in terms of Beltway politics but as a necessary move to give those charged with protecting the American homeland the power and resources it needed to do the job.

The Bush administration and Congress became locked in a serious political dispute over Homeland Security. As the conflict progressed, the political advantage was going to Congress. The Office of Homeland Security had not gotten off to a strong start. Positions were unfilled, and press accounts suggested that Ridge was not being consulted by other bureaucracies in their decision making on terrorism. Congress was also set to begin hearings into the performance of the intelligence community leading up to the terrorist attacks of 9/11. The star witness was to be an FBI whistle-blower who charged that the Bureau mishandled warning intelligence about those attacks. This revelation strengthened the hand of those who were calling for a Department of Homeland Security. Just hours after these accusations were made and only days before the congressional hearing was to take place, the Bush administration switched directions and endorsed the general concept of a Department of Homeland Security. In introducing his new plan, Bush again turned to symbolism, asserting that his proposal represented the most extensive reorganization of the Federal government since the 1940s.[4] Significantly, as we shall see, FBI and CIA intelligence activities were left virtually untouched by this reorganization. The Department of Homeland Security would not incorporate any of their activities, nor would it receive raw intelligence from them.

President Bush used similarly expansive and symbolic language two years later in signing the Intelligence Reform and Terrorism Prevention Act of 2004 that created the position of director of National Intelligence, calling it the "most dramatic reform of our nation's intelligence capabilities since President Harry S. Truman signed the national Security Act of 1947. Under this law our vast intelligence enterprise will become more unified, coordinated, and effective."[5] Establishing the position of Director of National Intelligence (DNI) had been one of the principal recommendations of the 9/11 Commission. In reality the Bush administration had shown little interest in having it come into existence.

With its attention riveted on waging the war against terrorism first in Afghanistan and then in Iraq, the Bush administration showed little interest in

retrospective post mortems on how 9/11 came about. It preferred that such inquiries wait on the successful conclusion of the war on terrorism. Initially this position succeeded. It was only after victory in Afghanistan that in December 2001 Senators Joseph Lieberman (D-CT) and John McCain (R-AZ) introduced legislation to bring an independent investigatory commission into existence. The Bush administration argued this was unnecessary because the House and Senate had now agreed to their own separate investigations. Finding that the terms of reference to these investigations were too restrictive, the families of the victims of the terrorist attacks continued to lobby for an independent bipartisan investigation. On November 27, 2002, the Bush administration and the Republican-controlled Congress agreed. Of particular concern to the administration and its supporters was that the 9/11 Commission would issue a negative report in the midst of the 2004 presidential campaign. To prevent this occurrence, the administration set a May 2004 reporting date and followed a policy of noncooperation with the commission. Vigorous lobbying by the families of the 9/11 victims and negative press coverage compelled the administration into first cooperating more fully with the commission and then agreeing to its request for a two-month extension. When the commission's report and recommendations were made public in July 2004, Democratic presidential candidate John Kerry quickly endorsed all of them and urged rapid action, leaving Bush with little choice but to endorse the report as well. As was the case with establishing a Department of Homeland Security, however, we shall see that creating the position of Director of National Intelligence amounted to far less than the imagery and rhetoric of major reform suggested.

Symbolic politics is not a one-time affair. It requires constant attention and reaffirmation. It is thus no surprise that the imagery of a war against terrorism has been a constant feature of the Bush administration's rhetoric before, during, and after the 2004 presidential campaign. Here the symbolic need exists to reassure the public not only that the structure of the intelligence community has been strengthened but that progress is being made. Two symbolic moves were made in this direction in 2005. Both came on the heels of public reports issued by members of the 9/11 Commission criticizing the administration for failing to enact crucial reforms. In one move, President Bush sought to refocus attention on the war against terrorism by announcing that the United States and its allies had disrupted ten serious terrorist plots since 9/11. Bush mentioned Osama bin Laden by name five times in his speech and asserted that groups inspired by Al Qaeda were trying to "enslave whole nations and intimidate the world." In another move, in late October, Director of National Intelligence John Negroponte publicly released the new National Intelligence Strategy of the United States. In doing so he observed that this document "shows Congress and the public our commitment to building an intelligence community that is more unified, coordinated, and effective.[6] Ten goals were identified for the intelligence community, including bolstering the growth of democracy, countering terrorism, and preventing the spread of weapons of mass destruction. Previous versions of this document had been secret.

Third, symbolic politics was used by the Bush administration to deflect criticism for intelligence failures in the lead-up to the Iraq war, especially as they related to the charge that Iraq possessed weapons of mass destruction, a charge that was central to the administration's case for involvement. Central to this strategy was restricting the terms of reference given to bodies looking into these intelligence failures. The Senate Select Intelligence Committee investigated and reported its conclusions in July 2004 and stated that nearly every finding in the National Intelligence Estimate released prior to the war was wrong. As part of the agreement by Republicans and Democrats on the committee, the Senate's investigation was divided into two parts. Part I, reported here, dealt only with the quality of prewar intelligence. The investigation was not permitted to examine how intelligence was used by the Bush administration. The administration's handling of intelligence was to be Part II of the investigation. As 2005 ended, Part II had yet to begin, and Republicans and Democrats on the committee were sparring over the need to hear testimony from administration officials.

A second effort a deflecting attention from the administration to the intelligence agencies came with the terms of reference assigned to the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, also known as the Silberman-Robb Commission, after its co-chairs, Judge Laurence Silberman and former Senator Charles Robb (D-VA). Bush initially resisted efforts to establish such a commission. He changed his position in early February 2004 following the late January resignation of UN chief weapons inspector David Kay and his subsequent testimony to Congress that "we were almost all wrong" about Iraq's weapons program.[7] Bush had argued that creating a commission to look into this issue was premature and should wait on a more exhaustive search for weapons of mass destruction. But now fearful that the White House would lose control over the issue, Bush endorsed a commission but indicated that it would look at intelligence on weapons programs in Libya, Iran, and North Korea as well. He also indicated that he would appoint all of its members. This move angered congressional Democrats, who argued that the commission could no longer be considered independent.

Unlike the 9/11 Commission, whose deliberations the administration had failed to control, the Silberman-Robb Commission held closed-door hearings rather than public ones. It was also not authorized to examine how policy makers used the intelligence they received. The Commission released its report on March 31, 2005. Where the 9/11 Commission stated that President Bush saw repeated warnings about a potential terrorist attack prior to 9/11, the Silberman-Robb Commission concluded that the intelligence community was "dead wrong" in most of their assessments.[8] Press accounts describe Silberman and Robb standing next to Bush at the public release of the report looking like bodyguards. The report mentions the CIA 1,567 times, the White House eight times, and Vice President Dick Cheney twice.

Finally, symbolic politics can be used to place responsibility for future problems on others. Consumer safety alerts, foreign travel advisories, drug warning

labels, and the like all say to citizens that the government is doing its job and now you must do yours. This is very much the case with issuing warnings about terrorist attacks. Lawrence Freedman notes that by communicating threat warnings, governments are able to shift responsibility for dealing with the risk of terrorism from governments to citizens, who are then the ones who make the decision on whether to ride the subways, go to work, or open their mail.[9]

As examples of this tendency, we have the October 2005 decisions to place police officers on every train, to have major shows of force at transportation centers in New York City, and to close the Baltimore Harbor Tunnel. All decisions were made in the aftermath of the London terrorist bombings in 2005, and the intelligence used consisted almost entirely of tips that a terrorist attack was possible in the immediate future. In the Baltimore case, the tip was described as uncorroborated. In the New York case, the threat was dismissed by Department of Homeland Security officials almost as soon as the alert was announced. On a more general level we have the color-coded alert system put in place by the Department of Homeland Security. Six times between its introduction after 9/11 and the presidential election of 2004, the system went into an orange or elevated alert level. Although issuing warnings holds the potential for shifting responsibility away from policy makers, it also has risks, especially when threats fail to materialize. Under these circumstances, policy makers are again trapped by their own symbols and run the risk of being accused of politicizing a situation or alarmism.

For intelligence, three consequences follow from the policy makers' desire to at least at a symbolic level protect themselves from charges that they are not doing their jobs. First, policy makers will demand greater specificity from intelligence than is possible. They will want the intelligence community to engage in fortune-telling.[10] One can see this outlook in President Bush's comment that the August 6, 2001, President's Daily Brief titled "Bin Laden Determined to Strike in US" did not contain specific enough information to take action.[11] Second, in the absence of concrete intelligence, policy makers tend to place greater emphasis on worst-case speculation about potential vulnerabilities and what terrorists might do rather than on the limited intelligence on hand about what terrorists are doing or planning. Finally, it heightens the tendency to engage in "sweepstakes" intelligence where the rush to a bottom-line conclusion takes precedence over sound analysis.[12] Taken together, these three tendencies work against the credibility of intelligence warnings over terrorist attacks but address the political imperative of shifting blame.

RESOURCE POLITICS

By its very nature and purpose, symbolic politics is a highly visible enterprise. Far less visible is the second political game or contest played out in Washington, DC: resource politics. Where the president is the principal political player in the symbolic politics arena, Congress and bureaucratic forces dominate

resource politics. Successful symbolic politics actually provides a cover that shields this political game from public view by encouraging the general population to turn its attention to other matters because public statements, laws, investigations, or administrative reforms have taken place that have addressed the problem. The struggle against terrorism is no exception. Speaking of the 9/11 Commission's call to create a powerful Director of National Intelligence and locate the office in the White House, Congressman Jack Murtha (D-PA) commented in September 2004 that "public indifference will make Congress able to resist changes [to the intelligence community]."[13] Presidents traditionally have not been active players in these political arenas because they care less about reorganization than do legislators and bureaucrats and frequently employ them as bargaining chips.

Resource politics are concerned with the basic fiber of organizations: their structure, budgets, and areas of jurisdiction. All were key areas of contention in intelligence policy in Washington after 9/11 with the creation of the Department of Homeland Security and the post of director of National Intelligence.[14] As noted in the discussion of symbolic politics, they both were hailed as significant accomplishments in improving the quality of intelligence and winning the struggle against global terrorism. It bears noting, however, that as the reorganization process came to an end, no intelligence agency was abolished. Instead, the number of intelligence bureaucracies increased.

We can see the central role played by resource politics in setting up the Department of Homeland Security and the corresponding lack of importance of attached to intelligence concerns by the two struggles that began and ended this political contest. The policy debate began over whether a Cabinet-level Department of Homeland Security or an Office of Homeland Security in the White House should be created. This is a structural issue, and at its heart was the ability of Congress to influence how its funds were spent and who would run the department. A White House Office of Homeland Security would be beyond its reach, but not a Department of Homeland Security. The final policy debate was over the degree of civil service protection to be afforded to personnel assigned to the new department and the power of the Secretary of Homeland Security. Under Bush's proposal, the secretary would have the ability to reorganize the Department of Homeland Security without congressional approval as well as great flexibility in hiring and firing employees. It would have subjected only fourteen of twenty-eight senior officials to senatorial confirmation to hire and fire individuals and change their job responsibilities. The battle over implementing a new personnel system did not end with passage of the legislation creating the department. In August 2005, a U.S. District Judge argued that the system undermined employees' collective bargaining rights. Another judge issued a similar ruling in February 2006 over an attempt to extend such a system to the Defense Department.

As created, the Department of Homeland Security had three primary missions: (1) to prevent terrorist attacks within the United States, (2) to reduce the vulnerability of the United States to terrorism, and (3) to minimize the damage

and assist in the recovery from terrorist attacks that do occur here. To accomplish these objectives twenty-two different agencies with some 170,000 employees were brought together in the new department. When President Bush publicly embraced the concept of a Department of Homeland Security in spring 2002, many inside and outside the administration speculated that it would become the primary intelligence center for the war on terrorism. Even the language establishing it suggested a major intelligence role. "Except as otherwise directed by the president the secretary [of Homeland Security] shall have such access to all information including reports . . . and unevaluated intelligence relating to threats of terrorism."[15] The reality proved to be quite different on both accounts.

The FBI and CIA were largely unaffected by the establishment of the Department of Homeland Security. Also remaining outside the new unit were the National Security Agency, the Defense Intelligence Agency, and the Northern Command, which is charged with the defense of American territory.

From the very outset, FBI Director Robert Mueller and Director of Central Intelligence (DCI) George Tenet spoke out against any rapid, major overhaul of the intelligence community, as did senior active and retired intelligence officials. Their opposition and uncertainty in Congress over how to proceed led to a decision to postpone intelligence reorganization and focus on reorganizing other aspects of Homeland Security, such as border and transportation protection, immigration, and disaster preparedness.

With intelligence agencies not subject to reorganization, the Department of Homeland Security became confined to the status of a consumer of intelligence and not a producer. Both the FBI and CIA pressed for strict limits on the information they had to share with the new department. One Senate aide close to the reorganization process stated that "there is real friction among these agencies. A lot of people want to put Homeland Security in a little box and not share much with them."[16] By mid-July Tom Ridge, still in his capacity as director of the White House Office of Homeland Security, was saying that the new department would limit its intelligence work to preparing warnings and leaving the central task of collecting intelligence to the FBI, CIA, and the Department of Defense intelligence agencies. Homeland Security was to be a coordinating center with access to the analytical production and information-gathering capabilities of the federal government. By the end of 2002, the administration's position retreated to the point where Ridge, now Secretary of Homeland Security, would only have access to unevaluated raw intelligence when he could make a case for it under yet-to-be-determined procedures.

These institutional and procedural arrangements did little to address the problem of intelligence sharing that the 9/11 Commission identified as a major deficiency in its report. Not only was the Department of Homeland Security limited in its access to intelligence from key agencies, but several units incorporated into its structure, notably the Coast Guard, Secret Service, Customs Service, and Immigration and Naturalization Service, retained their intelligence collection divisions.

The 9/11 Commission issued its report on July 22, 2004. Its central recommendation was the establishment of the position of Director of National Intelligence. This individual would oversee all-source national intelligence centers, serve as the president's principal intelligence advisor, manage the national intelligence program, and oversee the component agencies of the intelligence community. Included in his powers would be the responsibility for submitting a unified intelligence budget, appropriating fund to the intelligence agencies, and setting personnel policies for the intelligence community. The Director of National Intelligence's office would be in the White House.

The proposal to create a Director of National Intelligence, or DNI, became part of the Intelligence Reform and Terrorism Prevention Act of 2004. The House and Senate passed different versions of the bill with the Senate bill more closely following the 9/11 Commission's call for a strong DNI. The House bill provided for a far less powerful director. Under the Senate bill, the CIA director "shall be under the authority, direction, and control" of the national intelligence director. In the House version, the CIA director would only "report" to the National Intelligence Director. The House bill also only gave the National Intelligence Director the power to develop budgets and give "guidance" to intelligence community members. The Senate bill stated that he or she would "determine" the budget. The Senate bill would also make the intelligence budget public, require that most of the Director's high-ranking assistants be confirmed by the Senate, and create a civil liberties panel to prevent privacy abuses. Were the House version to prevail, which it largely did, some senators warned that Congress and the president would be creating a Potemkin Director of National Intelligence.

By fall, the House and Senate were deadlocked. Key opposition came from House Republicans led by Duncan Hunter (R-CA), chair of the House Armed Services Committee, who was adamant that the Pentagon should not loose control over its intelligence budget and that the overall intelligence budget should remain secret. To the consternation of the families of the victims of the 9/11 attacks and in the face of their pubic calls for action, President Bush remained on the sidelines as the battle dragged on. In fact, the administration from the outset had shown little interest creating the position of the position of DNI as outlined by the 9/11 Commission and was opposed to placing this office in the White House. Though the president did not speak out against the 9/11 Commission's recommendations, some argue he moved quietly to blunt the intent of the reforms through the issuance of executive orders and memos that in some cases did little more than reaffirm the system as it existed, including the secretary of Defense's operational control over defense intelligence agencies and intelligence priorities and in other cases advanced the commission's recommendations to established bureaucratic interests in a nonthreatening manner.[17]

Visible bureaucratic opposition to the 9/11 Commission's version of a DNI emerged soon after its report was released. Ridge opposed the idea, stating, "We don't need an intelligence czar."[18] Along with Secretary of Defense Donald

Rumsfeld and National Security Advisor Condoleezza Rice, he cautioned against moving too quickly. He also echoed Rumsfeld's warnings about creating a new layer of intelligence bureaucracy. Rumsfeld reportedly "blasted" the 9/11 Commission's report in classified hearings and stressed that centralizing intelligence outside of the Pentagon's control might undermine the military's ability to conduct the war against terrorism by placing barriers between Washington and battlefield commanders. The chairman of the Joint Chiefs of Staff, Gen. Richard Myers, made the same point in a letter he sent to congressional leaders. He asserted that if the Pentagon were to lose control of its spy satellites, troops on the ground would be endangered.

To these arguments were added partisan political concerns. Many Republicans in the House remained angry over what they considered to be the hostile treatment that administration officials received by the 9/11 Commission and the platform it provided to Bush's critics.[19] Republican opposition led by Hunter forced Speaker of the House J. Dennis Hastert to hold a Republican-only meeting in November to try to salvage a compromise bill. He failed, with Hunter winning an agreement that any bill should contain language that "directs the president to write regulations that protect the chain of command" regarding intelligence gathering aircraft and satellites.

In its final version, the Intelligence Reform and Terrorism Prevention Act of 2004 passed by Congress and signed by Bush followed far more closely the restricted vision of the Pentagon and its allies than it did the 9/11 Commission in establishing the DNI. Title I of the act stipulated that the DNI not be located in the executive office of the President. It gave the DNI the power to "develop and determine" an annual budget for the national intelligence program based on budget proposals provided by the heads of intelligence agencies and departments. The DNI is to ensure the "effective execution" of the annual budget and "monitor the implementation and execution of the National Intelligence Program." After consulting with department heads, the DNI is authorized to transform or reprogram a maximum of $150 million and no more than 5 percent of an intelligence unit's budget in any one fiscal year, but he or she may not terminate an acquisition program. He or she is also given the power to develop personnel policies and programs in consultation with the heads of other agencies and elements of the intelligence community.

Resource politics does not end in Washington with the passage of legislation but continues on a daily basis. Its effects at the Department of Homeland Security came into clear focus with its response to Hurricane Katrina. From the outset, fears were raised that the Federal Emergency Management Agency (FEMA) would experience a reduction in its ability to cope with natural disasters in the United States as a result of being placed in an organization whose primary mission was counterterrorism. Intelligence is not immune from these problems. In January 2006, Secretary of Homeland Security Michael Chernoff filled the position of chief intelligence officer with CIA veteran Charles Allen. Prior to his appointment, the position was vacant for seven months. Some half a dozen candidates

turned down the position in 2003 when the Department of Homeland Security was set up. Moreover, the intelligence fusion center that was to bring together intelligence from all sources had been overtaken in importance by establishing the position of DNI and creating a National Counterintelligence Center in his office.

In April 2005, the Silverman-Robb Commission, now acting as a private watchdog organization over intelligence reform, warned Bush to expect existing intelligence agencies to try to undermine the authority of the new DNI. Modernization plans being put forward by the FBI and CIA were described as a "business as usual approach to intelligence gathering."[20] Evidence on this last point was not long in coming. In May 2005 it was revealed that the two army analysts whose work was key to the faulty argument that the aluminum tubes sought by Iraq were part of a nuclear weapons program had received job performance awards for the past three years. The Silverman-Robb Commission had criticized their work as a "serious lapse in analytic tradecraft" because they did not seek out confirming or disconfirming information from the Energy Department or other intelligence agencies on the matter. In October, new CIA Director Porter Goss announced that he would not hold any current or former agency officials, including former CIA Director George Tenet, responsible for pre-9/11 intelligence failures, despite a recommendation by the CIA's inspector general that he convene an accountability board to judge their performance.[21] He had supported such a review when he served as chair of the House Select Intelligence Committee but now cited a desire to avoid hurting the agency. Inspector generals in the State Department, Justice Department, and Defense Department conducted similar reviews and declined to take disciplinary action against anyone.

Other evidence surfaced in 2005 that supported the commission's fears. In June the FBI, under pressure from the White House and Congress, agreed to let DNI John Negroponte help select the FBI's intelligence chief. Veterans within the agency had resented this move as an unprecedented infringement on the FBI's independence. At the same time, press reports indicated that FBI Director Mueller had taken steps to prevent deeper changes at the FBI by undertaking a series or reorganization measures in thee areas of collection and intelligence analysis. For example, the FBI moved 96 percent of its intelligence budget into units not under the jurisdiction of the DNI.

September brought a public relations embarrassment to the CIA as Robert Richer, the second-highest ranking officer in the Directorate of Operations and a Goss appointee, resigned and testified before the Senate committee about morale problems within the agency and Goss's lack of leadership and vision. The next month it was announced that in spite of recommendations by the 9/11 Commission that responsibility for human intelligence be transferred to the DNI, the CIA would remain as the chief coordinator of overseas spying by intelligence agencies. A National Clandestine Service within the CIA was to be created under Goss. It would supervise and coordinate spying but not direct the espionage activities of the FBI or Department of Defense intelligence agencies. Though located at the CIA, the new National Clandestine Service and all overseas human intelligence

collection programs will be overseen in the DNI's office by his deputy, Mary Margaret Graham, a former CIA intelligence official who left the Agency because of Goss.

The Intelligence Reform and Terrorism Act allowed the DNI to transfer up to 100 people from other intelligence agencies, including those in the Pentagon, but only in consultation with relevant congressional committees. The agreement reached with Congress at the time was that consultation meant approval from these committees. In June 2005 it was agreed that the House Armed Services Committee would not have veto power over personnel transfers. Instead Negroponte agreed to meet personally with Hunter to discuss any moves involving Pentagon personnel.

Resource politics potentially also has a second but more varied impact on those who produce intelligence. Richard Stoltz, former head of the CIA's clandestine service, suggests that the process of adding more layers to the intelligence bureaucracy will lead to a wait-and-see and risk-averse attitude among intelligence officials.[22] These are precisely the traits that drew so much criticism from the 9/11 Commission and other studies. At the same time, the process of redirecting resources, creating new units, and seeking to imbue them with a sense of urgency and purpose to their mission may also embolden some to act in ways that transgress the bounds of permissible behavior. After 9/11, the CIA came under pressure to capture members of Al Qaeda and their supporters. Renditions, the process of secretly capturing a suspect and transferring them to another country for interrogation, became a favored tool in the war on terrorism. Identifying candidates for rendition involved collaboration between analysts and operations officers sifting through tips and other pieces of circumstantial information as to a person's politics or identity. An estimated 3,000 people were captured. Unfortunately, not all of them had a connection with terrorism. Mistakes were made because of the fear of missing a case. And, in the process, the vetting and evaluating information suffered. It was "the Camelot of counterterrorism."[23]

AGENDA POLITICS

Policy makers are attracted to intelligence out of self-interest. They want to succeed, and to the extent that intelligence helps them succeed, they seek it out and use it. As one former diplomat noted, "I could not afford to read intelligence papers because this or that intelligence agency was empowered to produce them. . . . I could only read intelligence products tailored to help me through my substantive schedule."[24] This basic truth holds several important implications for intelligence. First, intelligence does not determine policy. Intelligence professionals recognize this. It is one ingredient in the mix of factors that determine what U.S. foreign and national security policy will be. The struggle against global terrorism is no exception. As Lawrence Freedman notes in speaking of the Iraq war, "This was not an intelligence driven crisis. The [9/11] attacks changed the

terms of the security debate . . . [policy] drew on intelligence information but could rarely be refuted or confirmed in a definitive manner."[25]

Second, intelligence is not always welcomed. Often it is inconvenient.[26] Typically policy makers seek to keep options open as long as possible, but the logic of intelligence is to close off options. Particularly problematic is intelligence that questions the wisdom of a policy after policy makers have publicly committed themselves to it. Intelligence may also be discounted when it suggests that a potential problem exists at a time when policy makers are focused on other issues. Again the struggle against terrorism provides examples. Planning within the State Department, the CIA, and nongovernmental organizations suggested that the rebuilding and occupation of Iraq would not follow the model of Germany or Japan (as administration officials suggested) but would be more difficult and require a much larger military force that was being planned for. These warnings were shunted aside.[27] The same can be said for the administration's response to doubts within the intelligence community about the soundness of the intelligence on which its pre-war policy rested; because the incoming Bush administration's agenda did not include terrorism as a prominent concern, attempts by Clinton administration holdover Richard Clarke and others to warn the administration about Al Qaeda fell largely on deaf ears.[28] For that matter, terrorism was also not a major issue in the Clinton administration. Prior to 9/11, the most comprehensive National Intelligence Estimate on terrorism was published in July 1995.

Third, to the extent that policy makers disagree over policy intelligence will become contested and competitive. Not only will policy makers seek out intelligence that supports their policy positions or undermines that of rivals, they will also seek to control its distribution. In some cases this will mean denying rivals access to it. In other cases it will mean going public with intelligence. Efforts by Bush administration officials to seek out supportive evidence in the struggle against terrorism prior to the Iraq war are well chronicled. Vice President Dick Cheney regularly visited CIA headquarters and challenged analysts on their sources and conclusions. Retired CIA official Michael Scheuer comments that the CIA received repeated inquiries from Undersecretary of Defense Douglas Feith's office at the Pentagon about Iraq–Al Qaeda links, causing the CIA to review over 70,000 documents.[29] Rumsfeld and Feith established the Office of Special Plans within the Defense Department to provide an alternative source of intelligence that would support their position.

The administration also sought to control access to intelligence. Defending its Iraq policy in 2005, the Bush administration argued that Congress had seen the same intelligence it had prior to the war. Yet the administration had far more intelligence available to it and did not share all it possessed. Doubts within the intelligence community were not shared, such as those expressed by the National Security Council four days before President Bush's 2003 State of the Union address, where he made the case for war against Iraq. The NSC had called for additional intelligence to support the claim that Saddam Hussein possessed chemical, nuclear, or biological weapons. In contrast to Director of Central

Intelligence George Tenet, who called the case for war "a slam dunk," the national intelligence officer for strategic and nuclear programs called the case "weak."[30] Similarly, doubts raised by a Defense Intelligence Agency analysis of the reliability of the administration's principal source establishing a link between Al Qaeda and Iraq were not shared nor reflected in Bush's October 2002 statement that "we know Iraq and al-Qaeda have had high level-contacts going back a decade."

Beginning in August 2002 and continuing through to the eve of war, the administration began a sustained and well-orchestrated campaign to promote public support for war against Iraq.[31] Central to this campaign was the release of intelligence (or references to intelligence) that supported its case. That month Cheney asserted that he was convinced Saddam Hussein possessed weapons of mass destruction. In support he cited information from defectors, including Hussein's son-in-law. Also in August, a White House Iraq Group under the direction of Chief of Staff Andrew Cord was set up to ensure that a unified front was being given by the administration on the need for war. In September, President Bush made several public references to Iraq's effort to obtain nuclear material and intelligence support for that assertion. In October he announced that Iraq was reconstituting its nuclear weapons program and that satellite photographs support this conclusion. He also asserted that the United States had discovered through intelligence that Iraq has a growing fleet of unmanned aircraft that might be targeted on the United States. In his January 2003 State of the Union address, Bush stated that the British government had learned of Iraqi efforts to obtain significant quantities of uranium from Africa. The next month, Secretary of State Colin Powell told the United Nations that his presentation of Iraqi efforts to obtain nuclear weapons was based on "solid intelligence." Twice more before war began, in March 2003 President Bush asserted that the United States possessed intelligence that "left no doubt" about Iraq's threat.

The fourth implication for intelligence of policy makers approaching it in a self-interested fashion is that they tend to view intelligence as a tool or instrument of policy. Intelligence is not supposed to have policy views of its own. It exists to serve them. Their basic approach is that they want "more, better and faster."[32] But in reality, intelligence officials are no more united in their views than are policy makers. The dividing lines separating intelligence officials are not necessarily partisan in the sense of Republican versus Democrat or realist versus neoconservative although such differences do exist. They are more likely to be centered on questions of institutional perspectives, control over information, the proper analytical frameworks employed, and definitions of professionalism. Thus, just as with policy makers, it is often necessary to find common ground to advance policy. In the case of the struggle against global terrorism, this common ground was the charge that Saddam Hussein possessed weapons of mass destruction. As Paul Wolfowitz acknowledged, "only the WMD issue had legs."[33] It was the only issue around which the bureaucracy could agree.

The failure to recognize that intelligence is not by definition neutral in its origins or infinitely malleable in its uses but that it reflects the thinking of

individuals embedded in organizations that contain their own political dynamics can set the stage for a particularly bitter brand of agenda politics—one that pits the White House against the portions of the intelligence community. The primary weapons at the disposal of the disaffected segments of the intelligence community are leaks. The recipients of these leaks tend to be the media or members of Congress. Their purpose is to alter the complexion of the political landscape by bringing other groups into the political fray that might otherwise not be aware that a policy is being contested or even under discussion. In addition to principled disagreement over policy decisions, self-interest plays an important role in the decision to leak intelligence. Policy makers come and go, but intelligence agencies are permanent. Recalling the post-Vietnam experience of the American military, those who leak may fear that their agencies will bear the blame for policy failures, excesses, and illegalities long after the policy makers who ordered them have left Washington.

This is the pattern of Washington politics that emerged with the beginning of the occupation and reconstruction of Iraq. Leaks from the intelligence community and military personnel provided the impetus for revelations about Abu Ghraib prisons, the practice of secretly capturing and incarcerating suspected terrorist suspects abroad, the use of torture as an interrogation device, and electronic spying on American citizens in the United States. In each case, these revelations succeeded in widening the circle of those participating in the policy debate. Most notably it brought renewed attention to Senator McCain, a former prisoner of war and a potential Republican presidential candidate who opposed the use of torture. Leaks also brought European leaders into the policy debate as information about secret CIA renditions in Eastern European countries occurred on the eve of Secretary of State Rice's 2005 trip there.

For its part, the Bush administration continued to make secret intelligence public on a selective basis to further its position. DNI Negroponte released an inflammatory letter allegedly written by Ayman Zawahari just as President Bush was giving a speech on Iraq defending the administration's policy. In an October 6, 2005, news conference, Bush announced that ten unidentified Al Qaeda terrorist plots had been disrupted by the United States and allied intelligence agencies since 9/11. When pressed on the subject by reporters, the administration later released a list of those incidents. Intelligence officials commented off the record that the administration had overstated the gravity of those plots and that most were far from being in a position to be carried out.

ACCOUNTABILITY POLITICS

To whom is intelligence responsible? As we have just suggested, from the point of view of policy makers, intelligence is responsible to them. They expect intelligence organizations to provide them with information and assessments that will allow them to succeed. The conventional wisdom in Washington is that

Porter Goss was made director of the CIA in 2004 to bring it under control and end the series of anti-administration intelligence leaks emanating from it. Goss would not be the first Director posted to the CIA for that purpose. He brought with him highly partisan staffers from the House Select Intelligence Committee. In his first months in that position, between thirty and ninety senior CIA officials left, including some whom Goss had appointed to key positions, and someone who worked on the Bush-Cheney election campaigns was placed in charge of the CIA's public affairs unit. Goss also issued a memo to CIA employees (soon leaked) in which he stated "as agency employees we do not identify with support, or champion opposition to the administration or its policies."[34]

Intelligence officials are well aware that executive branch policy makers are not the only ones interested in the performance of the intelligence community. Congress though its powers of the budget, appointment, and oversight has a constitutionally defined role in evaluating and assessing its performance. The media is also interested in intelligence both for its ability to provide a good story and because of its fourth estate role as a watchdog for the people over governmental action. Also active in the area of oversight, but generally playing a much more limited role in holding intelligence agencies responsible for their actions, are private sector interest groups, such as the Electronic Privacy Information Center, which aggressively pursues national security–oriented freedom of information questions.

Secrecy is an obvious and major impediment to the ability of political actors, outside of the small group in the executive branch who make national security policy, to judge the performance of intelligence. But it is not the only factor affecting the ability and willingness of Congress, the media, or interest groups to scrutinize intelligence agencies and personnel and hold them accountable for their actions or inaction. Three other factors, all rooted in Washington politics, also play major if not more important roles. They are deference, partisanship, and self-interest.

The 9/11 Commission characterized congressional oversight of intelligence as "dysfunctional," a situation that can be traced to the three traits just noted.[35] Deference was long visible in the approach that Congress brought to oversight during early years of the Cold War. The national consensus focused on the need to combat communism, coupled with the widely held view that intelligence was an instrument of foreign policy to be exercised by the president at his discretion. During this period, congressional oversight served more to protect the CIA and other agencies than make them accountable for their actions. It was only in the mid-1970s, after revelations of CIA involvement in the coup to bring down Salvador Allende's government in Chile and spying on American citizens inside the United States, that congressional oversight became aggressive with the establishment of the Church and Pike Committees in the Senate and House, respectively. In the wake of the investigations carried out by these panels, each body established Select Intelligence Committees for purposes of continued oversight. They largely followed a model that stressed bipartisanship and

deference to the president and his use of intelligence, with investigations being restricted to a examining problems only after they occurred rather than engaging in anticipatory or preventive oversight.

Deference to the president began to lessen during the Reagan years as the administration talked of "unleashing" the CIA and its Central American policies increasingly divided Republicans and Democrats. During the Clinton presidency, Congress (with Republicans leading the way) forced unwanted programs on the administration in the form of appropriating money for covert action programs against Saddam Hussein. In both administrations, as well as during Carter's term, the opposition party openly and successfully challenged the president's nominee to head the intelligence community. Deference returned briefly in the wake of the 9/11 terrorist attacks but soon faded as the United States moved from war in Afghanistan to war in Iraq. Partisanship became particularly intense in the House. Porter Goss, who chaired the House Select Intelligence Committee and was himself a retired intelligence officer who served in the clandestine service, had long acted as a protector of the CIA. Now he moved aggressively to protect the president. He often described the CIA as a mismanaged bureaucracy. He publicly supported the administration's position on weapons of mass destruction, and he blocked investigations into pre-war intelligence and the treatment of prisoners at Abu Ghraib as well as belittled the notion of an investigation into the leaking of undercover CIA official Valerie Plame's name to the press (linked by a special prosecutor to Lewis "Scooter" Libby in Vice President Cheney's office). During the presidential campaign, Goss also criticized Kerry's stance on intelligence in a speech on the House floor.

The 9/11 Commission rejected calls for tinkering with the system and urged a wholesale change that would establish a strong oversight committee in each chamber or a single joint committee. Congress reacted warily to the proposed reforms even while making support public statements. Of particular concern to legislators was the notion of giving one committee power over both setting program priorities and budget authority. This would produce a reduction in influence of the Appropriations, Armed Forces, and Foreign Relations committees. Senate Appropriations Chair Ted Stevens (R-AK) commented on the thrust of the 9/11 Commission calls for centralizing congressional authority: "I don't think it will fly."[36] House Appropriations Committee Chair C. W. Young (R-FL) observed that combining spending and authorization powers in one committee "is not part of this proposal" in discussing the House's response to the 9/11 Commission's plans. A Republican aide stated more bluntly that any such plan "doesn't have a snowball's chance in hell" of taking effect.

The same three factors emerge in media oversight of intelligence. Deference can be seen in how the press reports on intelligence. What the public tends to focus on are the sensational headlines of domestic spying, renditions, and the treatment of prisoners. Less often noticed is that the media is frequently in contact with the administration about the details of these stories and is sensitive to its concerns. In a November 2005 story revealing the covert prison system set

up to hold and interrogate suspected terrorists outside of the United States without restrictions, the *Washington Post* agreed with a request from senior administration officials not to identify the Eastern European countries involved.[37] The next month, the *New York Times* reported on the program of domestic spying that President Bush had secretly authorized following the 9/11 attacks.[38] The paper reported that it had delayed publishing the story for one year after meeting with the White House and that some information that administration officials had argued could be useful to terrorists was omitted. When it was released, charges of partisanship were quickly raised. The story surfaced just as the Senate was nearly a final vote on extending the USA-PATRIOT Act. A compelling case for self-interest in the timing of the story can be made by pointing to competition between the *New York Times* and the *Washington Post* in breaking such stories and the imminent publication of a book on domestic spying by the article's author, James Risen.

For a brief period of time, one public affairs interest group played a key role in accountability politics. Its behavior deviated from the pattern of deference, partisanship, and self-interest exhibited by Congress and the media. After its report was issued on July 22, 2004, the members of the 9/11 Commission disbanded and formed a nonprofit organization, the 9/11 Public Discourse Project, to fulfill what they saw as the commission's original mandate of guarding against future terrorist attacks and promote a national debate on how future attacks can be prevented. To that end, the 9/11 Public Discourse Project issued a series of report cards from September to December 2005 on the extent to which the commission's recommendations had been acted on. While seeking to be nonpartisan, the negative tone of its evaluation (one A–, twelve B's, nine C's, twelve D's, five F's, and two incompletes) struck a partisan chord in Washington. The 9/11 Public Discourse Project ceased operation on December 31, 2005, with its ultimate impact on intelligence and the struggle against terrorism unclear.

CONCLUSION AND SYNTHESIS: DOMESTIC INTELLIGENCE GATHERING

To the casual observer, Washington politics frequently appears to be a game without rules, rhyme, or reason. It seems messy, unfocused, and unprincipled. On closer inspection, a different picture emerges. Reoccurring patterns to politics can be found. They are symbolic politics, resource politics, agenda politics, and accountability politics. National security policy is not exempt from these patterns. As discussed here, they are very much alive in intelligence policy. Not all of these political games or contests are equally visible. Each has its own inner dynamics and central set of political actors. These political games or contests are not self-contained. Activity in one feeds on and is influenced by the politics in the others. Washington politics becomes particularly intense and combative when simultaneous activity is occurring in all four political games or contests. Such

was the case in late 2005 to early 2006 in the dispute over domestic spying on Americans as a means of gathering intelligence in the global struggle against terrorism.

In this case, agenda politics first came into public view. Controversy erupted in mid-December 2005 when the *New York Times* reported, on the basis of information leaked to it, that in February 2002 President Bush signed a secret order authorizing the National Security Agency (NSA) to monitor phone calls and other communications (such as faxes and e-mails) inside the United States by Americans identified by the NSA as having some connection to Al Qaeda or potential terrorist activities.[39] Published estimates placed the number of Americans being eavesdropped on at any one time as up to 500 and that all told, the number of Americans spied on may have reached into the thousands. The NSA, in turn, provided information to the Defense Intelligence Agency and others for use in carrying out its surveillance of people inside the United States. President Bush reportedly was deeply involved in the oversight of the program, reviewing it every forty-five or sixty days and reauthorizing it some thirty-six times.

The *New York Times* story broke the day before the Senate was to vote on reauthorizing the USA-PATRIOT Act. A key point of debate was whether the provisions of this act went far enough in protecting the civil liberties of Americans. The story appeared to have a significant impact and many senators expressed concern about the warrantless wiretapping. The next day by a vote of fifty-two to four-seven, with four Republicans voting with all but two Democrats, the Republican-controlled Senate refused to end the filibuster, signaling a setback for the act. Just days before, in an effort to ensure its passage, the Bush administration reversed its position and endorsed McCain's bill to ban the cruel, inhumane, and degrading treatment of prisoners in its custody. After extensive debate in the new year, Congress passed the renewed USA-PATRIOT Act on March 9.

The controversy that raged was not primarily over the value of this intelligence-gathering effort, although such questions were raised by some. Recall that what investigations of pre-9/11 intelligence revealed was not a failure to obtain intelligence per se but the inability to integrate it so that a meaningful pattern could be deciphered. After 9/11, a 2002 Senate Select Intelligence Committee report commented that "only a tiny fraction of the daily intercepts are actually ever reviewed by humans,, and much of what is collected gets lost in the deluge of data."[40] Experts on terrorism noted that terrorists were already well aware of the risks of phone, e-mail, and fax communications. They were now relying on ground couriers and the World Wide Web. The public was not overwhelmingly alarmed over domestic spying on Americans in the United States. The USA-PATRIOT Act had already given the FBI broad new powers to gather information on Americans. A January 2006 *Washington Post*/ABC News public poll found that almost two-thirds of Americans believed that the government's antiterrorism efforts were intruding on the privacy of American citizens, but less than one-third felt that this was unjustified.[41]

At the core of the issue was President Bush's authority to authorize this program on his own. And this moved intelligence politics squarely into the arena of symbolic politics with the outcome determining in large part which side would have the upper hand in the overall political contest. The president defended the program on the grounds that it was "limited, "a vital tool in the war on terrorism," and "critical to saving American lives." Most significant, he also stated that it was "consistent with U.S. law and the Constitution."[42] In making this last assertion, Bush was echoing the position taken by then Attorney General John Ashcroft who signed a brief on September 22, 2002, stating that "the Constitution vests in the President inherent authority to conduct wireless intelligence surveillance of foreign powers or their agents and Congress cannot by statue extinguish that constitutional authority."[43] Ashcroft's argument made no distinction between U.S. citizens or suspected foreign agents. In 2005, Attorney General Alberto Gonzales asserted that the administration's domestic eavesdropping was derived from the September 14, 2001, joint resolution authorizing the president to use "all necessary and appropriate force" to defeat Al Qaeda and the president's inherent powers as commander in chief. The Justice Department continued this line of argument, stating that because espionage is "a fundamental incident in the use of military force," even though it was not specifically mentioned, it was authorized by the resolution.[44] As the controversy grew, Bush engaged in symbolic politics again when he sought to redefine the program as "terrorist surveillance" and publicly presented an account of an Al Qaeda plot to crash a commercial jetliner into a Los Angeles skyscraper after 9/11. The significance of the revelation was quickly countered by unnamed intelligence officials who questioned whether the plot was anything more than loose talk.

Opponents countered with an argument heavily rooted in symbolism as well: American civil liberties were being violated, the rule of law had been broken, and neither Congress nor the Constitution provided such powers to the president. The Fourth Amendment to the U.S. Constitution protects citizens from unreasonable searches and seizures and stipulates that warrants can only be issued with probable cause. Opponents of Bush's policy assert that this prohibition has been interpreted by the courts to require a warrant and probable cause. Moreover, the Supreme Court has rejected the argument that national security considerations override this requirement. Opponents also challenged the stated limited nature of this program. The National Counterterrorism Center maintains a list of international terrorism suspects or those who might be providing them with aid. In early 2006, 325,000 names were on that list. Duplicate entries may reduce the total number of individuals listed to some 200,000. The number of U.S. citizens on the list has not been revealed. Names are provided by the CIA, NSA, FBI, and others and are given to the Transportation Security Administration and other agencies.[45]

Opponents continued that the rule of law was violated by Bush's failure to obtain permission from the U.S. Foreign Intelligence Surveillance Court to conduct surveillance on Americans inside the United States. This eleven-judge body, all of whose members were selected by the late Chief Justice of the Supreme

Court William Rehnquist, was set up by the Foreign Intelligence Surveillance Act (FISA) that was passed in the 1970s after revelations of widespread spying on Americans by the military and the NSA in the name of rooting out communist influence on the anti–Vietnam War movement. According to the Justice Department, in 2004 the secret court approved 1,754 warrants. By one account it had received over 5,600 requests since 2001 and rejected only four.[46] Provisions of the act also allow for emergency wiretaps without the consent of the court for up to seventy-two hours. The Bush administration's position was that FISA was not relevant because the September 14, 2001, resolution constitutes a statute that by the terms of the act can override its provisions. One of the judges resigned in protest following revelations that the program existed and the presiding judge of the secret court requested a briefing on why it was not consulted. Finally, former Senate Majority Leader Thomas Daschle (D-SD) stated that the Bush administration had requested war-making authority from the Senate in discussions over the wording of the September 14, 2001, resolution and that it was rejected.

The political battle over what symbolic reference points were to be used in judging the appropriateness of this intelligence-gathering policy set the stage for a renewed round of accountability politics. As noted above the Foreign Intelligence Surveillance Court was ignored. Only its presiding judge was informed, and she raised concerns in private that this program could undermine the secret court's work if information so obtained was later used to acquire warrants on terrorist suspects. In fact, twice since 9/11 the FISA court was told that information obtained by this program may have been improperly used to obtain wiretap warrants. Vice President Cheney informed leaders of both parties about the program after it started and later the administration informed key members of Congress. These congressional briefings are given to the Gang of Eight, the leadership of the House and Senate and the intelligence committees. Staff members are not present, and those briefed are prohibited from discussing the information with other members of Congress, including those who serve on the intelligence committees. The administration contends that with these briefings, Congress gave its approval to the domestic spying program. After it became public, John D. Rockefeller IV (D-WV), the ranking Democrat on the Senate Select Intelligence Committee, revealed that in 2003 he sent a letter to Cheney stating that the briefings were unsatisfactory. The letter stated, "Given the security restrictions associated with this information, and inability to consult staff or counsel on my own, I feel unable to fully evaluate, much less endorse, these activities."[47] House Minority Leader Nancy Pelosi (D-CA) expressed concerns about the legality of NSA domestic spying in a letter to Gen. Michael Hayden, who as head of the NSA in October 2001 briefed the House Select Intelligence Committee on its broadened domestic operations. She wrote, "I am concerned whether and to what extent the National Security Agency has received specific presidential authorization for the operations you are conducting."[48] Hayden's response remains classified, but an intelligence official indicated that he had not been referring to the new NSA domestic spying program.

Although the content of these briefings is the subject of debate, it is clear that congressional oversight was carried out with deference to the administration and far more in the spirit of putting out fires (which had not yet occurred) than patrolling for dangers. When the program became public, Congress quickly moved out of principle and self-interest to reassert its oversight powers as both Democrats and Republicans called for hearings and previously secret correspondence was made public. Partisanship was not completely absent, as many Republican members of Congress staunchly defended the program and the president's right to implement it. Cheney went so far as to suggest that the debate over spying on terrorists ought be an issue in the upcoming congressional campaign. The possibility that the NSA's domestic spying program might become an issue that Republicans could seize on led two leading congressional Democrats to acknowledge its importance in the war against terrorism while rejecting Bush's legal authority to act without congressional approval.

In additional to maintaining its right to conduct such a surveillance program, the administration also sought to deflect attention away from the question of presidential authority by returning to symbolic politics. Bush asserted that the story of the day was not the domestic intelligence-gathering program but the war in Iraq. The administration also called attention to the illegality of the leak and launched a Justice Department investigation into who leaked the information announcing in January 2006 that the NSA's inspector general would conduct an investigation into the matter. Critics observed that Bush had already maintained that the NSA's general counsel and inspector general had approved the domestic spying program, so little should be expected from this probe.

Lying beneath the surface of this controversy we can also find resource politics. During the Cold War, the NSA collected intelligence on the Soviet Union through electronic intercepts and controlled much of the intelligence community's secret budget. This mission no longer exists. The war on terrorism provided an opportunity for the NSA to reinvent itself, but doing so was not without challenges. As a former NSA director observed, "We've gone from chasing a slow-moving, technologically inferior, resource poor nation-state to chasing a communications structure in which an al Qaeda member can go into a storefront in Istanbul and buy for $100 a communications device that is absolutely cutting edge, and for which he has had to make no investment for development."[49]

The NSA has long been authorized to monitor international phone calls and e-mails of American citizens without a warrant when they originate overseas. Secret NSA intelligence gathering in the United States was limited to communications intercepts involving foreign embassies and missions and only then with a warrant. The major exception was when an individual was suspected of being an "agent of a foreign power" or a member of a terrorist group. Otherwise it generally fell to the FBI to carry out domestic eavesdropping operations. The expansion of the NSA's role after 9/11 was implemented with an eye to achieving results and not the imposition of controls. It was mid-2004 before voices of concern were raised. At that time, elements of the program were suspended and

others recast after concerns were raised by national security officials and the head of the Foreign Intelligence Surveillance Court.

This was not the only expansion in domestic intelligence-gathering activities after 9/11. Also in late 2005, it was revealed that the Defense Department's new counterterrorism agency, the Counterintelligence Field Activity (CIFA), had expanded its efforts from a coordinating and oversight body into one with operational responsibilities. Its Directorate of Field Activities became responsible for disrupting adversaries, running roving patrols around military bases, and conducting surveillance on potentially threatening people and organizations inside the Untied States. CIFA also manages data bases that include Talon reports that consist of raw and unverified information collected by the military on suspicious activities. Talon reports are known to include information on peaceful civilian protests and demonstrations. In November 2005, the CIFA was given authority to task the domestic U.S. investigations and operations of the military counterintelligence units.

As promised by Senator Specter, hearings on the NSA's domestic surveillance program began in February 2006 after Congress returned from its winter recess. An all-out White House lobbying campaign plus a late-found willingness to brief House and Senate committees on the programs slowed down the momentum that had built for an investigation. The Senate rejected a Democratic attempt to launch an investigation into the matter through a procedural maneuver, which allowed time for a Republican working group appointed by Majority Leader Bill Frist (R-TN) to explore ways of changing the law to accommodate NSA's policy. Democrats were quick to criticize the formation of an all-Republican committee.

White House spokesman Scott McClellan sought to further calm the waters by outlining a new White House position. He stated that the NSA program does not require "congressional authorization" but that the administration is "open to ideas regarding legislation."[50] Two competing ideas became the center of attention. One, endorsed by the White House, was sponsored by Representative Mike DeWine (R-OH). It would provide additional congressional oversight for the NSA's domestic spying program but exempt it from FISA oversight. Such oversight would most likely come from a subcommittee of the intelligence committee with the full committee restricting itself to a review and modernization of the FISA. The second, opposed by the Bush administration, was introduced by Specter. It would require the NSA to obtain prior permission from the Foreign Intelligence Surveillance Court.

NOTES

1. For a CIA statement describing the intelligence cycle, see http://www.odci.gov/cia/publications/facttell/intelligence_cycle.html.

2. Murray Edelman, *The Symbolic Uses of Politics* (Urbana: University of Illinois Press, 1964).

3. Michael Howard, "What's in a Name? How to Fight Terrorism," *Foreign Affairs* 81 (2002), pp. 8–13.

4. *Weekly Compilation of Presidential Documents* (June 21, 2002). From 2002 Presidential Documents online via GPO Access at http://www.gpo.gov/nara/nara003.html; *Weekly Compilation of Presidential Documents* (December 17, 2004), from 2004 Presidential Documents online via GPO Access, http://www.gpo.gov/nara/nara003.html.

6. Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States*: *Transformation through Integration and Innovation* (October 2005), Washington, DC.

7. http://www.Washingtonpost.com (January 28, 2004).

8. Katherin Shrader, "WMD Commission Releases Scathing Report," *Washington Post* (March 31, 2005), p. A1.

5. Lawrence Freedman, "The Politics of Warning: Terrorism and Risk Communication," *Intelligence and National Security* 20 (2005), pp. 379–418.

6. Shlomo Gazit, "Estimates and Fortunetelling in Intelligence Work," *International Security* 4 (1980), pp. 36–56.

11. See Dan Eggen, "Memo Not Specific Enough, Bush Says," *Washington Post* (April 12, 2004), p. A1.

12. Jack Davis, *Improving CIA Analytical Performance: Strategic Warning* (Washington, DC: Sherman Kent Center for Intelligence Analysis, Occasional Papers 1:1, Central Intelligence Agency, September 2002).

13. Charles Babington, "Hill Wary of Intelligence Oversight Changes," *Washington Post* (September 12, 2004), p. A5.

14. For a historical perspective on such politics, see Amy Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, CA: Stanford University Press, 1999).

15. Walter Pincus, "Lesser Intelligence Role Seen for Security Dept.," *Washington Post* (July 18, 2002), p. A6.

16. Ibid.

17. Michael Turner, "Intelligence Reform and the Politics of Entrenchment," *International Journal of Intelligence and Counterintelligence* 18 (2005), pp. 383–97.

18. Dan Eggen and Dafna Linzer, "9/11 Commission Offers Critiques on Many Fronts," *Washington Post* (July 22, 2004), p. A1.

19. Helen Fessenden, "The Limits of Intelligence Reform," *Foreign Affairs* 84 (2005), p. 110.

20. Walter Pincus, "FBI, CIA Proposal to Retool Called 'Business as Usual,' " *Washington Post* (April 15, 2005), p. A6.

21. Dafna Linzer and Walter Pincus, "CIA Rejects Discipline for 9/11 Failures," *Washington Post* (October 6, 2005), p. A1.

22. Quoted in David Ignatius, "Danger Point in Spy Reform," *Washington Post* October 21, 2005, p. A3.

23. Dana Priest, "Wrongful Imprisonment: Anatomy of a CIA Mistake," *Washington Post*, December 4, 2005, p. A1.

24. Robert D. Blackwill and Jack Davis, "A Policymaker's Perspective on Intelligence Analysis," in *Strategic Intelligence: Windows into a Secret World,* eds. Loch K. Johnson and James Wirtz (Los Angeles: Roxbury, 2004), p. 122.

25. Lawrence Freedman, "War in Iraq: Selling the Threat," *Survival* 46 (2004), p. 38.

26. Jack Davis, *Strategic Warning: If Surprise Is Inevitable, What Role for Analysis?* (Washington, D.C.: Sherman Kent Center for Intelligence Analysis, Occasional Papers 2:1, Central Intelligence Agency, January 2003).

27. James Fallows, "Blind into Baghdad," *Atlantic Monthly* 293 (January/February 2004), pp. 52ff.

28. Richard Clarke, *Against All Enemies* (New York: Free Press, 2004).

29. Anonymous [Michael Scheuer], *Imperial Hubris* (Washington, DC: Brassey's, 2004).

30. The "slam dunk" remark is from Bob Woodward, *Plan of Attack* (New York: Simon & Schuster, 2004), p. 249; the "weak" remark from Walter Pincus, "Prewar Findings Worried Analysts," *Washington Post* (May 22, 2005), p. A1.

31. Glenn Hastedt, "Public Intelligence: Leaks as Policy Instruments—The Case of the Iraq War," *Intelligence and National Security* 20 (2005), pp. 419–39.

32. James Simon Jr., "Managing Domestic, Military, and Foreign Policy Requirements: Correcting Frankenstein's Blunder," in *Transforming U.S. Intelligence,* eds. Jennifer Sims and Burton Gerber (Washington, DC: Georgetown University Press, 2005), p. 154.

33. Lawrence Freedman, "War in Iraq: Selling the Threat," *Survival* 42 (Summer 2004), p. 26.

34. Robert Dreyfuss, "The Yes-Man," *American Prospect* 16 (November 2005), pp. 18–24.

35. On congressional oversight see L. Britt Snider, "Congressional Oversight of Intelligence After September 11," in Jennifer Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005), pp. 239–58, and Loch K. Johnson, "Governing in the Absence of Angels: On the Practice of Intelligence Accountability in the United States," in *Who's Watching the Spies?* eds. Hans Born, Loch K. Johnson, and Ian Leigh (Washington, DC: Potomac Books, 2005), pp. 57–78.

36. This and the other quotations in this paragraph are from Charles Babington, "Hill Wary," p. A5.

37. David Johnston and Carl Hulse, "C.I.A. Asks Criminal Inquiry Over Secret Prison Article," *New York Times* (November 9, 2005), p. A18.

38. James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times* (December 16, 2005), p. A1.

39. Eric Lichtblau and James Risen, "Spy Agency Mined Vast Data Trove, Officials Report," *New York Times* (December 24, 2005), p. A1.

40. Michael Hirsh, "The NSA's Overt Problem: So Many Conversations, So Few Clues to the Terrorist's Chatter," *Washington Post*, January 1, 2006, p. B1.

41. Dan Beltz and Claudia Deane, "Differing Views on Terrorism," *Washington Post,* January 11, 2006, p. A4.

42. Lisa Rein, "Bush Defends Spying Program as Necessary to Protect U.S.," *Washington Post* (January 2, 2006), p. A2.

43. Barton Gellman and Dafna Linzer, "Pushing the Limits of Wartime Powers," *Washington Post* (December 18, 2005), p. A1.

44. See "Legal Authorities Supporting the Activities of the National Security Agency Described by the President," Department of Justice (January 19, 2006).

45. Walter Pincus and Dan Eggen, "325,000 Names on Terrorism List," *Washington Post,* February 15, 2006, p. A1.

46. Suzzane Spaulding, "Power Play," *Washington Post,* December 25, 2005, p. B1.

47. Charles Babington and Dafna Linzer, "Senator Sounded Alarm," *Washington Post* (December 20, 2005), p. A10.

48. Dafna Linzer, "Secret Surveillance May Have Occurred Before Authorization," *Washington Post* (January 4, 2006), p. A3.

49. Quoted in Hirsh, "The NSA's Overt Problem."

50. Charles Babington and Carol Leonnig, "Senate Rejects Wiretapping Probe," *Washington Post*, February 17, 2006, p. A6.

7

THE INTELLIGENCE WAR AGAINST GLOBAL TERRORISM

RICHARD L. RUSSELL

AMERICANS WERE HORRIFIED THAT THEIR INTELLIGENCE COMMUNITY (IC) failed to detect and disrupt the Al Qaeda surprise attacks of September 11, 2001. They rightly ask, "How is it possible that the intelligence community, which costs American taxpayers tens of billions of dollars per year, so miserably failed in protecting citizens and the homeland?"

The IC should have better been prepared to warn of Al Qaeda operations because the terrorist organization had been waging a war against the United States for some time. Al Qaeda bombed the American embassies in Kenya and Tanzania in 1998 as well as attacked the U.S.S. *Cole* in Yemen in 2000. These attacks should have signaled loud and clear that Al Qaeda had declared war on the United States, but American naiveté fueled the view that terrorist attacks were more a problem for law enforcement than for the military. Both civilian policy makers and the military hierarchy resisted moving the United States to a war footing to take head on the threat posed by Al Qaeda.[1] In response to the African embassy bombings, the United States could only muster half-hearted retaliatory cruise missile strikes against Al Qaeda–affiliated positions in Afghanistan and Sudan, which did little to blunt the network's capabilities to strike again against the United States.

The CIA, too, had not moved to a wartime footing to tackle Al Qaeda. Director of Central Intelligence George Tenet had warned in a December 1998 memorandum to his key lieutenants in the IC that the United States was at war with Al Qaeda and that he wanted no resources spared for the fight.[2] But Tenet's bravado was not matched by resources. The team inside the CIA's Counterterrorism Center (CTC) in the run-up to 9/11 only had five analysts assigned to track global Al Qaeda operations.[3] A handful of analysts is hardly commensurate with Tenet's call

to "spare no resource." Within the CIA's Directorate of Operations (DO), responsible for collecting human intelligence, senior management believed that the Al Qaeda threat before 9/11 was being exaggerated and resisted assigning CIA resources to the problem, according to former White House official Richard Clarke.[4] The former head of the bin Laden unit in the CTC, Michael Scheuer, even believes that senior CIA officials "have made careers by keeping silent in the face of unfairness, avoiding risk, and refusing to make decisions."[5] The CIA's own inspector general has found senior CIA officials negligent for failing to competently orchestrate the Agency's resources against Al Qaeda prior to 9/11.[6]

But that, as they say, is all history. The challenge today for scholars, intelligence officers, policy makers, and the American public is to move beyond the blame game and take a hard, clear-eyed look at what went wrong. We need to find ways to sharpen the nation's intelligence capabilities for countering Al Qaeda—as well as loosely aligned affiliates and successor organizations that share a militant Islamic ideology and hatred of the United States, which they blame for most (if not all) of the failings of the Islamic world—in what regrettably promises to be a long-term struggle.

The term *terrorism* generates considerable debate and controversy, which sometimes boils down to the view that "one man's terrorist is another man's freedom fighter." Many observers in the United States tend to view operations conducted by terrorist groups against American military and diplomatic facilities and personnel as terrorist attacks, but they probably should be more accurately seen as insurgents using terrorist tactics to wage war. Today the news headlines are dominated by Iraqi insurgent use of terrorist tactics, especially roadside bombings, in their battle against American forces in Iraq. But in the past, other insurgent groups have used terrorist tactics against the United States, sometimes with nation-state sponsorship. Hezbollah, for example, benefited from Syrian and Iranian support in the 1980s in its bombings in Lebanon, which killed about 250 Marines and destroyed the American embassy in Beirut. The Saudi Hezbollah benefited from substantial assistance from Iran when it bombed the Khobar Towers in Saudi Arabia in 1996 and killed nineteen American servicemen.[7] In short, Al Qaeda is not the first militant Islamic movement to use terrorism against the United States, and they are not likely to be the last. To steer clear of that thicket of debate on the differences between terrorism and insurgency, this chapter views terrorism as the use of violence by transnational groups or organizations that is directed principally against civilians for political purpose.

The CIA has traditionally played the leading role in the IC along three major lines to support the president in the war on terrorism. First, the CIA runs human intelligence operations needed to penetrate the walls of secrecy behind which terrorists plot and plan against the United States. Second, the CIA performs analysis of terrorist groups to inform presidential decision making. And third, the CIA is also tasked to mount covert actions against terrorist groups to disrupt,

prevent, and preempt their operations. This chapter critically examines the CIA's past performance in each of these areas against the terrorist adversaries, draws some lessons learned, and makes recommendations for strengthening future performance. This chapter acknowledges that the CIA's traditional position as the premier intelligence service in the community has been eclipsed by the creation of the Director of National Intelligence (DNI) and will conclude with some thoughts on how the DNI should best orchestrate the reorganized IC.

STEALING THE TERRORISTS' SECRETS

The IC taps a wide and deep array of sources of information to understand international terrorism. The United States uses diplomats and defense attachés posted abroad to collect information. It relies on publicly available information, such as newspapers, periodicals, and websites to analyze terrorist group memberships, propaganda, recruitment, and ideology. The IC also is able to use satellite imagery to identify terrorist training camps and state support for terrorist groups. The United States, for example, in 1998 used many of these sources of intelligence to identify Al Qaeda training camps in Afghanistan for retaliatory cruise missile strikes for the bombing of the two embassies in Africa.[8] The IC also clandestinely acquires information on terrorist groups and their plans from human sources (human intelligence, or HUMINT) and from intercepting communications such as radio, telephone, and e-mail (signals intelligence, or SIGINT). The primary responsibilities for these HUMINT and SIGINT operations fall, respectively, to the CIA and the National Security Agency (NSA) in the IC.

The CIA's Directorate of Operations, which was recently renamed the National Clandestine Service (NCS), is charged with running human intelligence operations intended to collect strategic intelligence on American adversaries.[9] The CIA's core human intelligence collection mission is to steal secrets that adversaries want to hide from the United States, secrets that could adversely affect American national interests.

The CIA's operational tradecraft for running human operations was honed during the Cold War. The Agency's operational officers working abroad under cover had used a method of spotting, accessing, developing, and recruiting Soviet diplomats and military officers primarily by trolling the diplomatic cocktail circuit. Though this is a proven method of human collection, the CIA's human operations against the Soviet Union were, on balance, less than impressive. Before the entire stable of CIA spies in the Soviet Union were exposed to the Soviet KGB by traitor Aldrich Ames, the Agency only had about a dozen spies inside the Soviet Union.[10]

The method is now deeply ingrained into the institutional culture at the CIA, and it has been stubbornly difficult for the Agency to move toward contemporary international terrorists targets. A former CIA case officer who was in the Agency's training class as late as 1999, nearly a decade after the Cold War,

recalls that it was still focused on trolling the diplomatic cocktail party circuit.[11] Unfortunately, and quite obviously, members of Al Qaeda, Hezbollah, Hamas, Islamic Jihad, and their state sponsors in Syria and Iran do not regularly participate in diplomatic cocktail parties. Nor, for that matter, do the scientists and technicians with experience in weapons of mass destruction (WMDs) programs who might offer their talents to terrorist groups with or without the knowledge of their countries. Rogue Russian scientists trying to make a lucrative living are a particular problem on this score.

The CIA has done precious little to exploit alternative means of getting human intelligence information. Most notably, the Agency has a strong bureaucratic culture to run "agents in place" even though it has failed to do this with any consistency or reliability over a period of decades. The CIA and American security would much better off it the Agency were sparing no expense or effort to encourage defections from countries with pervasive and oppressive internal security apparatus, called "hard target" countries. The United States, for example, should be offering money and perhaps resettlement in the United States or the West for disaffected Al Qaeda and Hezbollah members and scientists and technicians laboring in North Korea's and Iran's suspected nuclear weapons programs, who all could offer significant intelligence to the United States. Dozens of defections would give CIA analysts snapshots of terrorist groups and plans, intentions, and capabilities, as well as disrupt WMD-related activities.

The CIA also significantly suffers in human operations against Middle East terrorist groups such as Al Qaeda and Hezbollah because it suffers from shortages of Arabic and Farsi speakers. Former CIA case officer Robert Baer lamented that he was one of only two Arabic speakers in the CTC when it was set up in the 1980s to track Hezbollah and Palestinian terrorist groups.[12] And judging from news reports today, the CIA is not gaining ground fast enough to address this gap. The chancellor of the University of California at Berkeley, for example, meet with CIA officials to discuss language capabilities and came away from the meeting with the understanding that "their needs are desperate."[13]

The CIA also is overly dependent on foreign intelligence liaison service information. Because the Agency lacks foreign language capabilities, it relies on foreign intelligence services, which do have hard languages such as Arabic and ethnic backgrounds needed to penetrate terrorists cells. The Senate-House investigation into 9/11 determined that the CIA is overly dependent on liaison reports and fails to deliver its own or "unilaterally" acquired human intelligence. It found that "the Intelligence Community depended heavily on foreign intelligence and law enforcement services for the collection of counterterrorism intelligence and the conduct of other counterterrorism activities. The results were mixed in terms of productive intelligence, reflecting vast differences in the ability and willingness of the various foreign services to target the Bin Ladin and al-Qa'ida network."[14] Unilaterally acquired intelligence is essential to compare and check against the information provided by foreign liaison services as well as other American sources of information.

There can be no gainsaying how important these liaison relationships are to human intelligence collection in the war on terrorism. But with that said, for all of the problems and shortcomings in the American intelligence community, they pale in comparison to the problems that plague many foreign liaison services. For example, these foreign services suffer from a deep subordination to vested policy interests, ingrained bureaucratic and cultural resistance to "speaking truth to power," personal fears of delivering bad news to their superiors, as well as worldviews—especially pronounced in the Middle East—that greatly hamper objective and critical analytic thinking and intelligence. There is also a significant risk that liaison services skew their human intelligence reports shared with the United States to influence the direction of American foreign policy. These tendencies all underscore the critical need for the CIA to acquire its own unilateral intelligence sources.

The NSA is charged with the responsibilities for intercepting the communications of terrorist groups. The United States has had better collection performance in strategic intelligence from the NSA than the CIA. Tragically, however, NSA operations against Al Qaeda appear to have suffered a major blow when word leaked by August 1998 that the United States was listening to Osama bin Laden's satellite telephone conversations, and he stopped using the satellite phone shortly after U.S. cruise missile strikes against his camps in Afghanistan in retaliation for the bombings of two American embassies in Africa.[15]

The NSA is now deeply embroiled in a domestic spying controversy with accusations that it was listening to American phone calls and e-mails domestically without the legal authority to do so.[16] Above and beyond today's news headlines, the NSA is up against the wall in reorienting its collection operations from the Cold War to the war on terrorism. Al Qaeda and other terrorist groups benefit enormously in the explosion in information and communication technology, and the NSA has not been able to keep pace. Al Qaeda can now purchase off-the-shelf encryption technology, making it difficult if not impossible for NSA to crack their communications. Al Qaeda can hide its communications in the billions of e-mails and cell phone calls made daily. And Al Qaeda operatives can easily and readily replace cell phones, making it extraordinarily difficult for the NSA to keep apace of small, nimble, and adaptive terrorist cells.

The shortcomings of CIA human operations and NSA communication interception operations were made painfully clear in the aftermath of the 9/11 attacks. The joint House-Senate investigation found that the CIA had no human agent placed inside Al Qaeda in a position to steal secrets on the 9/11 conspiracy.[17] Although the NSA did intercept some Al Qaeda communications related to the conspiracy, the intercepts were not sufficiently specific and not translated into English before the attacks because the NSA lacked the resources to translate all the communications it manages to intercept.[18] But even if these communications had been translated before 9/11, they would not have been sufficiently detailed to have allowed U.S. officials to wrap up the Al Qaeda cell that orchestrated the attack.

ANALYZING TERRORISTS INTENTIONS, PLANS, AND CAPABILITIES

Intelligence analysis does not hold the public's fascination nearly as well as human intelligence operations and covert action, which are the stuff of spy novels and adventure movies, but it plays no less a critical role in the war on terrorism. Even the best human intelligence and superb intelligence from other sources will come to naught if it not married with first-rate analysis.

The CTC has been the focal point for intelligence collection as well as analysis. The CTC was an exceptionally innovative organization that was created in the mid-1980s to grapple with the problems the United States was facing with Palestinian terrorism as well as Iranian-backed Hezbollah terrorism that was responsible for the bombings of the American embassy, the Marine Corps barracks in Beirut, and the kidnapping of American citizens, such as the CIA's station chief in the 1980s.[19] The creation of the CTC was a remarkable bureaucratic innovation because it located in one office both CIA case officers charged with running HUMINT operations with the CIA's Directorate of Intelligence (DI) analysts. The CIA had traditional fostered a bureaucratic barrier between case officers and analysts partly to protect disclosure of sources and methods, but the separation prevented the synergy of case officers working side by side with analysts. Analysts could identify blind spots and recommend avenues for case officers to gain access to individuals with access to information to fill intelligence gaps.

Despite these strengths, the CTC suffers from a lack of substantive analytic talent, a shortcoming that is a reflection of the CIA's entire analytic corps. The Senate-House inquiry discovered that "the quality of counterterrorism analysis was inconsistent, and many analysts were inexperienced, unqualified, undertrained, and without access to critical information. As a result, there was a dearth of creative, aggressive analysis targeting Bin Ladin and a persistent inability to comprehend the collective significance of individual pieces of intelligence."[20]

Notwithstanding these profound weaknesses, the CTC did indeed provide strategic intelligence warning to President Bush of the September 11 attacks. The CIA in its August 6, 2001, *President's Daily Brief*—a daily current intelligence document prepared for the president and his closest advisors—had warned Bush in an article titled "Bin Laden Determined to Strike in US."[21] The CIA's warning, however, was more a historical review than tactical intelligence needed to disrupt the conspiracy. In contrast, the FBI did have specific information coming from astute field offices in Arizona and Minnesota on suspected Al Qaeda members training on commercial aircraft, but Bureau headquarters lacked a robust analytic staff in Washington to "connect the dots."[22]

Although the strategic intelligence failure of 9/11 falls most heavily on the FBI, the CIA, for whatever reason, took the lion's share of public blame. As is the case with many reforms, the 9/11 Commission recommended changes that "threw the baby out with the bathwater" and recommended a new center under the auspices of the DNI for doing counterterrorism analysis, a recommendation

that President Bush accepted.[23] The new National Counterterrorism Center (NCTC), however, will likely be inferior to the old CTC because it will not benefit from shoulder-to-shoulder relationships with the CIA's case officers.

COVERTLY KILLING AND DETAINING SUSPECTED TERRORISTS

The collection of intelligence—via clandestine human sources, intercepted communications, and other means such as satellites and media monitoring—by far consumes the lion's share of the American intelligence community's budget, which now is running at $44 billion per year.[24] But public attention is captivated by covert action, which is designed to influence events abroad without exposing the hand of the United States, and special activities such as training foreign security services.[25]

These activities, which after many years tend to become publicly exposed, create political controversies in the United States and abroad. One of the largest covert action programs in the CIA's history was the military backing of the insurgency against the Soviet Union's occupation of Afghanistan during the Cold War. The CIA spent millions of dollars and provided tons of military arms and equipment to the Afghan insurgents over a period of years to substantially increase the costs of Soviet occupation and contributed to the Soviet decision to withdraw from Afghanistan. That less-than-covert war is heralded by CIA veterans as an exemplar of covert action that contributed to ending to the Cold War. Other commentators are not so sanguine and argue that the covert action program gave military training, expertise, and battlefield experience to militant Islamic extremists, who later went on to found Al Qaeda. The truth probably lies somewhere in between, but it is important to note that the United States never dealt directly with bin Laden during the Afghan war. Bin Laden's direct sponsors and benefactors were intelligence services of Saudi Arabia and Pakistan.[26]

Covert action has taken on an increasingly important role in the war on terrorism, which the public gets glimpses of by leaks. The CIA did a superb job in facilitating the U.S. Special Forces entry into Afghanistan in the 2001 war.[27] Covert actions such as the ones carried out in Afghanistan are carried out by the CIA and need to be authorized by a presidential order called a finding, which is shared with and approved by the House and Senate oversight committees to be legal in the American judicial system. Traditionally, the presidents have banned American assassination of foreign leaders under executive orders, a practice that has been perpetuated since President Ford's Executive Order 12333, which prohibited assassinations, a move to stem the tide of public criticisms against the CIA and the IC during a tumultuous period of history in American intelligence.[28] CIA Director Porter Goss recently told Congress in public testimony that the ban on assassinations by U.S. intelligence is still in force, but that it does not prohibit the CIA from killing terrorists.[29]

The CIA appears to be effectively using armed unmanned aerial vehicles (UAVs) to kill Al Qaeda operatives. The CIA has used armed UAVs to kill operatives in Yemen and Pakistan as well as in Iraq. "Several U.S. officials confirmed that at least 19 occasions since Sept. 11 on which Predators successfully fired Hellfire missiles on terrorist suspects overseas, including 10 in Iraq in one month last year [2005]. The Predator strikes have killed at least four senior Al Qaeda leaders, but also many civilians, and it is not known how many times they missed their targets."[30]

Some critics have faulted the CIA for falling to use the armed UAVs to target bin Laden or covert paramilitary operations to capture him prior to 9/11. The CIA's Directorate of Operations chief in 1998, for example, did not want to use his funds to sponsor a paramilitary operation to grab bin Laden from his farm in Afghanistan and "expressed concern that people might get killed" and that "the operation had at least a slight flavor of a plan for an assassination. Moreover, he calculated that it would cost several million dollars. He was not prepared to take the money 'out of hide,' and he did not want to go to all the necessary congressional committees to get special money."[31] Although civilians have been tragically killed in paramilitary operations, military strikes, or UAV attacks since 9/11, the strikes are probably still legitimate instruments of war—as long as there is a reasonable chance of killing Al Qaeda operatives and leaders who are sworn to kill as many American civilians and soldiers as they can as long as they live.

The CIA is also using covert teams to located suspected Al Qaeda operatives abroad—in areas where UAV attacks would not be politically viable options, such as in Europe—and in daring raids called renditions they sweep them off the streets and bring them to other countries for detention and interrogations. These operations have been embroiled in controversies. Italy, for example, is in a political uproar because a CIA team took a person off Italian soil.[32] Other European and Asian countries are in an uproar over the purported existence of a string of clandestine CIA detention facilities on their soil. The CIA also has been publicly condemned for blatant violations of the Geneva Conventions with the use of techniques that are commonly considered to be torture in its interrogations undertaken in U.S. military detention facilities in Afghanistan, Iraq, and Guantánamo Bay, Cuba.[33] These accusations include charges that the CIA is using a technique called water-boarding, which makes detainees believe they are drowning. Not only is this technique morally unacceptable, many professional interrogators judge that this technique produces bad intelligence because prisoners will say or make up anything to get interrogators to stop the water-boarding.[34]

The United States may have already fallen victim to this intelligence pitfall. According to journalist James Risen, the information the CIA got from debriefing one high-level Al Qaeda operational commander was fabricated because he wanted to stop water-boarding.[35] Another CIA detainee who was reported tortured after the CIA turned him over to Egyptian officials fabricated information on Iraq's links to Al Qaeda in the run-up to the 2003 Iraq war.[36]

STRENGTHENING INTELLIGENCE COLLECTION, ANALYSIS, AND COVERT ACTION FOR THE WAR ON TERRORISM

Lawyers could argue until the sun goes down whether water-boarding and other techniques the CIA is using constitute the legal definition of torture, but the average American using his or her common sense and moral compass would have little to no difficulty calling these techniques torture. And the American legalistic argument that Al Qaeda operatives are "enemy combatants" and not "prisoners of war" who are governed by the Geneva Conventions carries little weight with Americans and even less with the Middle Eastern populations, which the United States desperately needs to wean away from ideological support for Al Qaeda recruitment and operational support. Even the appearance of Geneva Conventions violations renders American calls for freedom and democracy in the Middle East as sheer hypocrisy and aids and abets our terrorist enemies by handing them ready-made justifications for their ruthless tactics, such as decapitating hostages. Even in its intelligence war on terrorism, the United States must uphold its own ethical standards and not stoop to those of the morally deprived barbarians it is fighting.

The CIA's use of paramilitary operations was a success story in the 2001 war in Afghanistan. But in the wake of the war, the 9/11 Commission recommended—on not very deep analysis or consideration—that these functions should all be controlled by the Pentagon and that CIA should get out of the business. The commission said, "Before 9/11, the CIA did not invest in developing a robust capability to conduct paramilitary operations with U.S. personnel. It relied on proxies instead, organized by CIA operatives with the requisite military training. The results were unsatisfactory."[37]

The recently announced Quadrennial Defense Review, which calls for a substantial beefing up of American Special Operations Forces, will likely work to further push the CIA out of paramilitary operations. The plan is to increase the number of special operations forces by 14,000 to about 64,000, the largest number since the Vietnam War, to fight small Al Qaeda cells dispersed across some eighty countries.[38] The Pentagon's new emphasis no doubt reflects in part the frustration of Defense Secretary Donald Rumsfeld over the lethargic response of the Special Forces to get into the 2001 Afghanistan war in comparison to the quick dispatch of CIA operatives into Afghanistan, which won high praise and respect from President Bush.[39] The push to remove the CIA from the paramilitary business will make sense as long as the Pentagon gives its Special Operations Forces room for operational ingenuity, a key ingredient of effective special operations. Unfortunately, creativity and ingenuity are often crushed by the weight of the Pentagon's bureaucracy.

The DNI, a post created by the president on the recommendation of the 9/11 Commission, will have his hands full trying to overcome the shortcomings of American strategic intelligence against terrorist groups. The DNI's activities so far have focused on recruiting a staff, leaving little time for substantive reforms

to address strategic intelligence shortcomings all too evident to the American public in the aftermath of 9/11. The DNI, not the director of the CIA, is now the president's principal intelligence advisor. The DNI has established the National Clandestine Service, the Open Sources Center, and centers under his wing for counterterrorism and counterproliferation, as well as named IC collection managers for Iran and North Korea.[40] There is little evidence to show that these steps are anything more than renaming old organizations, however, and adding some new ones to respond to calls for reform, while in practice doing little to qualitatively improve America's intelligence performance in the war on terrorism.

These bureaucratic fixes run the risk of creating a false impression that the United States has "corrected" of all its strategic intelligence shortcomings in the war on terrorism. But the real, root causes of past failures lie in the quality of human intelligence collection and analysis. The creation of the DNI and new national support offices do nothing directly to correct the bureaucratic culture and failed business practices that are stubbornly rooted at the grassroots level of the CIA. Until reforms and profound changes in managerial business practices change at this level, all the reorganizing and changing of the bureaucratic wiring diagrams at the senior most rungs of the U.S. intelligence community will amount to little more than rearranging the deck chairs on the *Titanic*.

NOTES

The views expressed are those of the author and do not represent the policy or position of the National Defense University, the Department of Defense, or the U.S. government.

1. For an insightful analysis of the political and military obstacles against moving to a war footing against Al Qaeda before 9/11, see Richard H. Shultz Jr., "Showstoppers: Nine Reasons Why We Never Sent Our Special Operations Forces after al-Qaeda before 9/11," *Weekly Standard* (January 26, 2004).

2. House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001* (Washington, DC, December 2002), p. 40. Hereafter referred to as the Joint House-Senate Inquiry.

3. Ibid., p. 59.

4. Richard A. Clarke, *Against All Enemies: Inside America's War on Terror* (New York: Free Press, 2004), pp. 205, 210.

5. Anonymous [Michael Scheuer], *Through Our Enemies' Eyes: Osama bin Laden, Radical Islam, and the Future of America* (Washington, DC: Brassey's, 2002), p. xiv.

6. Greg Miller, "CIA Plans No Discipline over 9/11," *Los Angeles Times* (October 6, 2005), p. A10.

7. For the most authoritative study of state sponsorship of terrorist groups, see Daniel L. Byman, *Deadly Connections: States that Sponsor Terrorism* (New York: Cambridge University Press, 2005).

8. On policy deliberations, see Clarke, *Against All Enemies*, pp. 184–89.

9. Walter Pincus, "CIA to Retain Coordinator of Overseas Spying," *Washington Post* (October 13, 2005), p. A4.

10. John Diamond, "CIA's Spy Network Thin," *USA Today* (September 22, 2004).

11. Lindsay Moran, "More Spies, Worse Intelligence?" *New York Times* (April 12, 2005).

12. Robert Baer, *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism* (New York: Three Rivers Press, 2002), p. 86.

13. Cited in Michael Janofsky, "Bush Proposes Broader Language Training," *New York Times* (January 6, 2006), p. A15.

14. Joint House-Senate Inquiry, p. 109.

15. Glenn Kessler, "On Leaks, Relying on a Faulty Case Study," *Washington Post* (December 23, 2005), p. A3.

16. On the controversy, see James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times* (December 16, 2005), p. A1.

17. Joint House-Senate Inquiry, p. 90.

18. Ibid., p. 205.

19. For an account of the innovative creation of the CTC by its founding chief, see Duane R. Clarridge with Digby Diehl, *A Spy for All Seasons: My Life in the CIA* (New York: Scribner's, 1997), pp. 321–29.

20. Joint House-Senate Inquiry, 59.

21. *The 9/11 Commission Report* (New York: Norton, 2004), pp. 260–61.

22. See the Joint House-Senate Inquiry, pp. 325–35.

23. For the recommendation to establish the NCTC, see *The 9/11 Commission Report*, pp. 403–6.

24. The budget figure was revealed by a senior official in the DNI's office in 2005. See Scott Shane, "Official Reveals Budget for U.S. Intelligence," *New York Times* (November 8, 2005), p. A18.

25. For an insightful discussion of the differences between covert action and special activities, see William J. Daugherty, *Executive Secrets: Covert Action and the Presidency* (Lexington: University Press of Kentucky, 2004), pp. 12–16.

26. For a fascinating accounts of CIA's covert action program in Afghanistan, see Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and bin Laden, from the Soviet Invasion to September 10, 2001* (New York: Penguin Press, 2004) and George Crile, *Charlie Wilson's War: The Extraordinary Story of How the Wildest Man in Congress and a Rogue CIA Agent Changed the History of Our Times* (New York: Grove Press, 2003).

27. See Gary C. Schroen, *First In: An Insider's Account of How the CIA Spearheaded the War on Terror in Afghanistan* (New York: Ballantine Books, 2005).

28. For a concise history of congressional oversight of the CIA and covert action, see Loch K. Johnson, "Presidents, Lawmakers, and Spies: Intelligence Accountability in the United States," *Presidential Studies Quarterly* 34, no. 4 (December 2004), pp. 828–37.

29. Shaun Waterman, "Goss Says CIA Ban Excludes Terrorists," *Washington Times* (March 25, 2005), p. A5.

30. Josh Meyer, "CIA Expands Use of Drones in Terror War," *Los Angeles Times* (January 29, 2006), p. A1.

31. *The 9/11 Commission Report*, p. 113.

32. In a reflection of the anger surrounding the case, an Italian judge ordered the arrest of thirteen suspected CIA officers who participated in the rendition operation in 2003. See Stephen Grey and Don Van Natta, "In Italy, Anger at U.S. Tactics Colors Spy Case," *New York Times* (June 26, 2005), p. A1.

33. For an insightful treatment of the CIA's covert activity and ethical dilemmas with maintaining prison facilities for renditioned individuals, see Dana Priest, "CIA Holds Terror Suspects in Secret Prisons," *Washington Post* (November 2, 2005), p. A1.

34. James Risen, *State of War: The Secret History of the CIA and the Bush Administration* (New York: Free Press, 2006), pp. 32–33.

35. Ibid., p. 33.

36. Douglas Jehl, "Qaeda-Iraq Link U.S. Cited Is Tied to Coercion Claim," *New York Times* (December 9, 2005), p. A1.

37. *The 9/11 Commission Report*, p. 415.

38. Greg Jaffe, "Rumsfeld Aims to Elevate Role of Special Forces," *Wall Street Journal* (February 18, 2006), p. A1.

39. Bob Woodward, *Bush at War* (New York: Simon & Schuster, 2002), pp. 53, 78–80, 88, 99.

40. John D. Negroponte, "Intelligence Reform: Challenges and Opportunities," 25th Jit Trainor Award Speech, Georgetown University, February 17, 2006.

8

INTELLIGENCE TO COUNTER TERROR

The Importance of All-Source Fusion

JENNIFER SIMS

FROM 1934 TO 1937, THE BRITISH GOVERNMENT collected suspicious communications from its monitoring station at Camberwell.[1] Peeling back the encryption with the help of a well-placed mole and several émigrés, the government discovered the existence of an illicit Soviet spying and covert action network operating on British soil. It appeared to involve senior politicians and established political organizations. Direction-finding equipment owned by the Army intercept station at Fort Bridgewoods, the Air Ministry at Waddington, and at the Royal Navy's receiver at Flowerdown established the location of the network's transmission sites. MI5 used this knowledge to begin surveillance of the broad-based network, penetrate it with human intelligence assets, and gain advance notice of illegal activities. These counterintelligence efforts eventually established that the illicit British cells were connected to Vienna, Shanghai, Prague, Copenhagen, Zurich, Paris, Spain, and the United States. All were directed by Moscow and coordinated through the operations of Comintern or Communist International. According to British historian Nigel West, this huge counterintelligence operation, which intercepted a total of 1,571 messages, disrupted Moscow's efforts to influence British elections "on a massive scale."[2]

This is the story of MASK—the code name for MI5's penetration of the Communist Party of Great Britain during the period between the world wars. Although the details of the story are worth rereading in the post–September 11, 2001, political context, just the facts summarized above suggest three truths about counterintelligence operations directed against networks: first, they involve intrusive domestic operations, often against domestically based groups designed to "disappear" within the societies in which they operate; second, they require patient accumulation of data over a lengthy period of time; and finally, they

depend on information fused from a variety of widely differing sources. These three ingredients, essential for such operations almost a century ago, are still important in the age of global, digitalized information flows and transnational threats. In fact, the new digital environment has made transnational crimes vastly easier to coordinate on a worldwide scale than was possible before World War II. It has also exacerbated a most serious challenge: governments (particularly democracies) attempting to stop terrorists are expected to do so without undermining the laws, representative principles, and informal confidences upon which a culture of democracy depends. Unfortunately, what Britain succeeded in doing against its domestic threat—to the satisfaction of the British public—was done even better within the militarized Nazi German state by Hitler's Gestapo and the Schutzstaffel, or SS ("Blackshirts"). If, as President Truman once promised the American people, we are not in the business of creating a Gestapo in this country, what are the proper limits of our counterintelligence business?

The purpose of this chapter is to examine the modern intelligence requirements for countering terror to appreciate this challenge in greater depth and develop a reasoned basis for balancing counterintelligence capabilities with civil liberties. What is meant by all-source data fusion in intelligence work, and how necessary is it against terrorists? How necessary are government-wide databases of digitalized information, and why does the idea of connecting them worry civil libertarians? If, as the post-9/11 commissions have suggested, one of the U.S. government's worst intelligence failures during this tragedy was the lack of adequate data fusion and analysis, what has been done about it, and can we do more without intolerable risks to our social and moral fabric?

To explore these questions, this chapter begins by considering the nature of the terrorists we face and the requirements for good intelligence operations against them. Historical examples will illustrate that there are lessons to be learned from the defeat of similar threats in the past, including the recurring ways in which challenges to civil liberties arise as democracies optimize intelligence in the name of security. Second, I run through the special opportunities and challenges modern technology presents. Third, I discuss an essential next step for democracies threatened by terrorists in their midst.

THE NATURE OF INTELLIGENCE AND COUNTERINTELLIGENCE IN THE AGE OF TERROR

As has been repeatedly pointed out, terrorism is a tool, not an adversary in and of itself. Yet adversaries who use this tool reveal much about themselves. They are ruthless, have strategies and tactics that require operational access to their victims, and they are able to organize in pursuit of their goals. Moreover, unless they are psychopathic, they use terror because they have no alternative that offers as much opportunity to win battles. Public access to national treasures and

freedom to organize are integral to Western democracies' most vital interests. Democracies intent on fighting adversaries who exploit openness to kill massively, risk undermining themselves. Countering such adversaries at the strategic level may require understanding their larger purposes to deflect, overcome, or undermine them. But to defeat them at the tactical level, one must deny them access, disrupt their ability to organize, or deny them their "victories" even if their tactics succeed. One must know what they are doing and either catch them at it or refuse to flinch—ideally, both. Intelligence, in any case, is essential.

The Role of Intelligence

Intelligence is best understood as the collection, analysis, and dissemination of information by parties in conflict or competition. What turns the simple pursuit of information into the business of intelligence is its purpose: gaining competitive advantage over adversaries.[3] This goal fuels the desire for specific, urgent, and often secret knowledge as well as a systematic way of obtaining it in time to win the contest. Given that the context is competition, such decision advantages can be acquired in two ways: by getting better information for one's strategy than one's opponents gain for theirs, or by degrading the competitors' decision making through denial, disruption, deception, and surprise.[4] This latter category of activity is called *counterintelligence*. More than just security, counterintelligence involves discovering what opponents think they need to know and then using this information to block, disorient, confuse, and ultimately beat them. In virulent or hostile competitions, increasing the speed of one's own decision making and the mobility of the decision makers may unbalance the opponent more than trying to discern and defend all the information believed to be critical to that opponent's strategy—a process that can actually slow decision making and cripple one's offense. Of course, the best way to protect an intelligence system is to own the adversary's intelligence system through the use of moles, double agents, and the like.

Gangs, bureaucrats, and football teams all use a form of intelligence to gain advantages over their competitors.[5] The more intense and lawless the competition, such as in international politics, the more secretive intelligence operations tend to become and the more decisive the potential advantages they offer. In fact, for states, intelligence can be more than a life or death enterprise; it can entail the end of nations and cultures.[6] For these reasons, secrecy is often viewed as a necessary component of national or transnational intelligence efforts. It is more accurate, however, to think of secrecy as an attribute of a relatively good intelligence effort—not an essential requirement for it. Some contestants' counterintelligence capabilities are so poor that they are not aware of what information they should protect to beat their adversaries. Or they believe their relative agility makes such protection unnecessary. Trying to defeat such opponents by only looking for secrets they protect would lead to failure. Intelligence must instead work to collect the information that provides the competitor with a decision

advantage over opponents—whether or not that information is secret—and to assume adversaries are doing likewise.

Arguably, a preoccupation with secrets cost the United States much before the devastation of 9/11. Although the terrorists' plans were indeed closely held, their operations were boldly open. Most used their true names when making airline reservations, used common addresses, and communicated on the Internet—not through privileged diplomatic pouches or hidden radios. The trick to catching them would have been to combine what we knew from the efforts of the Central Intelligence Agency (CIA) to track them overseas with what we could have known from the surveillance and unclassified information collected at home by the Federal Bureau of Investigation (FBI). Using classified sources to tip off the FBI and discern the unclassified information crucial for counterterrorist decision making is a critical part of the domestic intelligence enterprise.[7]

Traditionally, U.S. intelligence has used three types of collection to target opponents: technical intelligence (TECHINT), human intelligence (HUMINT), and open-source or unclassified intelligence (OSINT). TECHINT includes the collection of imagery, intercepted communications, electronic signals emitted by equipment, engineering data from captured electronics or weapons systems, and data from equipment or materials in the environment that leave signatures of their presence (such as radiation, effluent plumes, and noise) that trained analysts can discern using pre-existing data as reference.[8] The productivity of any of these collectors against a particular target will depend on that collector's access to the target's most vulnerable point. For example, if a network of spies uses wireless radios, picking up their electronic emissions (TECHINT) will be an effective way to find them; if they use couriers, human agents secretly opening the letters and packages (HUMINT) is likely to work best; if the adversary believes he is unobserved, collecting the names of those he visits from a phone book or the sites he visits while traveling as an ostensible tourist (OSINT) would be useful.

In any case, the best intelligence is obtained when the capabilities of all these collectors are quickly combined. Just as newspaper editors like to see multiple sources corroborating articles even from their best reporters, directors of national intelligence have greater confidence in intelligence that comes from multiple collectors. Better than simply hearing that Osama bin Laden has been sighted on a road in Pakistan would be seeing imagery of his convoy and receiving intercepts from his communications that each independently confirm the initial report.[9] As long as an opponent runs reasonably complex operations, some collectors will work best against certain aspects of those operations, whereas others will work best against the rest. Thus "all-source" collection can yield many pieces of a puzzle that analysts can then assemble, jumble up, and reassemble as the adversary moves, reacts to countermoves, and moves again.

Beyond corroboration, however, is the concept of collection boosting, in which the productivity of one collector depends on input from others.[10] The most obvious example of boosting within a single discipline is "direction finding" (DF), which may involve the use of multiple antennae to triangulate on a signal so that

it can be not only identified but also geo-located with some degree of precision.[11] During World War II, the SS paired up with the Gestapo and used DF to locate the wireless radios used by a network of Stalin's spies in Europe. To their great chagrin, these radios were found in Berlin—some next to the most sensitive government ministries.[12]

Of course, boosting also works among collection disciplines, such as the use of spies (HUMINT) to steal the codes of adversaries so that analysts working on intercepted communications (TECHINT) can overcome the encryption methods and read the content of the messages.[13] In fact, the more tightly integrated collectors are in the decision-making process, the more likely an adversary's spoofing of a collector will work to deflect or deceive one's own decision makers. Because securing collectors can be a costly and seemingly never-ending endeavor, one good way to compensate for inevitable vulnerabilities is to ensure collection is "constructively redundant"—that is, sufficiently all-source that one collector's vulnerability to spoofing will not lead to misperception or miscalculation.

This kind of constructively redundant all-source collection was a linchpin of the Allied strategy to defeat Hitler during World War II; it was employed, for example, to determine whether covert and clandestine collection operations had been compromised and specifically in the running of the famous British counterintelligence operation known as the Double Cross System.[14] But the history of Double Cross also alerts us to the inherent dangers of redundant collection systems: Because collectors improve the reliability of each other's products by offering independent corroboration, they depend on good system-wide counterintelligence so an adversary can't defeat or spoof one of them and thus sow ambiguity, uncertainty and confusion throughout an interlaced collection system. If systemic counterintelligence is weak, collectors have good reason not to share their "take" lest it become tainted. Poor counterintelligence can lead to system-wide failure even when the majority of collection endeavors are robust and productive.[15]

In some respects, then, the business of all-source data fusion for countering terrorism follows what has been done in a traditional sense against other intelligence targets. What makes the counterterrorism a particularly challenging endeavor is the terrorists' objective of committing stealthy crime—often on the victim's home soil. This means that law enforcement information, including information on U.S. residents or citizens living in close proximity to terrorists, may be important intelligence information that needs to be shared with decision makers at the federal level working to thwart terrorist activities on a nationwide scale. Law enforcement agents, dedicated to preserving the information for the purposes of arrest and prosecution, realize the need to pass the information over to these officials but do not always know the best and most secure ways to do so. At times, in fact, the most important decisions must be made very quickly by state and local officials if they are to prevent an impending attack. In these cases, circulating information to Washington for recycling into intelligence products could delay action rather than assist it. The problem thus becomes the very nontraditional one of fusing all-source intelligence for a cop on the beat.

Intelligence for Counterterrorism

In other words, what makes terrorists particularly difficult intelligence targets for traditional intelligence systems is that they organize as networks, insinuate themselves into open societies, and kill suddenly. Whereas traditional collectors were designed to penetrate governments located in state capitals or military deployments located on discrete battlefields, terrorists specialize in operating in small numbers and under the skins of their adversaries—that is, wherever they can do the most damage. They fashion themselves to look like their targets and burrow into society to lie in wait. In this sense they occupy the same moral space as assassins, but without an assassin's traditional limits on targeting. Deceit is part of terrorists' stock in trade, and innocents are their intentional victims. Often free of the vertical command structures of their more bureaucratic opponents, they achieve agility through compartmented operations, often using minimal communications. Their offensive operations are also crucial to their defense; by instilling fear and panic, terrorists create sufficient confusion to enable their swift escape. For many of these reasons, analysts have long argued that it takes a network to fight networked organizations, such as Al Qaeda.[16]

Unfortunately for democracies, counterterrorism requires gaining access to the enemy where he operates, including on one's own soil. And because terrorists do not operate against a national security establishment but against an entire society, they will not necessarily be focused on any particular city or on stealing secrets from traditional national security establishments. This means that it may be necessary but no longer sufficient to use forms of collection appropriate to the Cold War, when the enemy was a highly bureaucratized state, targeting Washington and using a command-and-control system stretching halfway around the world. To stop terrorists, information from traditional intelligence collectors will need to be combined with information collected by those disconnected to the traditional national security community. Hospitals may be the first to see a spike in disease associated with a biological weapons attack; police may be the first to bust a document forger or stop a car carrying explosives; customs agents at a port may be the first to notice discrepancies between the scan of a shipping crate and its official manifest; a landlord may be the first to notice his building's security system is detecting toxic gases; and a shopper may be the first to notice someone in a mall or store pushing a heavy baby carriage with no baby inside.

Against this kind of threat, time is of the essence, yet indications and warning may come from untrained people just doing their day jobs. The intelligence these domestic collectors acquire, moreover, will often need to be analyzed and provided back to them. After all, they are likely to be the decision makers best placed to stop the attack itself. The first 9/11 counterattack was, in fact, carried out by passengers on an airliner—once they knew from collecting intelligence over their cell phones what they were up against and what was at stake.

In the modern era of the Internet and the global reach of broadband communications, terrorists have new capabilities beyond the reach of any one country.

By piggybacking on this information system, bolstered by highly effective private encryption, transnational terrorist groups can communicate instantaneously and largely anonymously, even to the extent of sending sensitive information embedded in pictures on websites or in e-mails, a practice known as steganography. For this reason, the intelligence gained by other states and their private sector collectors may be as potentially valuable as intelligence collected unilaterally; much depends on the confidence a state has in its liaison relationships—confidence that should fluctuate more with the capabilities of that state's counterintelligence capabilities than with the number of its perceived friendships.

The overall picture, then, is of proliferating intelligence sources, increasingly complex all-source analysis, and a maddeningly contingent list of those decision makers who not only need the results but must get them in record time. Preparation of a terrorist attack might take years, but its execution or prevention may take only hours or minutes. As bad as this situation sounds, it is not all that new. As with today's terrorists, past plotters have threaded themselves through the fabric of the societies they planned to attack. Catholics, intent on overthrowing the Protestant Queen Elizabeth I and installing her Catholic cousin, Mary, Queen of Scots, were distinguishable from Elizabeth's loyalists only by their faith. Sir Walsingham, Elizabeth's Secretary of State and chief spymaster, nonetheless caught them.[17] Kaiser Wilhelm's saboteurs infiltrated German immigrant communities in the United States prior to World War I so that they would have cover for their mission to blow up weapons depots, warehouses, and storage facilities. They, too, were countered—this time by a network of British liaison officers and U.S. law enforcement personnel, assisted by the intermittent incompetence of the saboteurs themselves.[18] Successful counterterrorist intelligence operations such as these have generally employed well-known principles: collect multisource intelligence, tighten borders, tap liaison services, conduct deception operations, and enlist law enforcement to interdict and "turn" the criminals so frequently but superficially aligned with terrorists, such as forgers and money launderers.[19]

What makes the current, post-9/11 effort so much more difficult than in times past is the nature of modern technology. Technology has affected the counterterrorist mission in a number of ways. For example, experts have discussed at length how advances in weapons technologies have rendered the scariest forms of attack—biologically engineered germs, toxins, and nuclear explosive or radiological devices—feasible for small numbers of nonexperts to execute. Perhaps less well understood among the general population is the extent to which advances in communications technology permit terrorist networks to exchange messages and plan attacks on a worldwide basis and to do so almost instantaneously.

The development and widespread use of commercial surveillance technologies mean that information on a developing terrorist attack that is acquired by private citizens or local businesses can in theory be handed off rapidly to local and federal officials even though it is "owned" by others. Individuals outside the traditional national security community may therefore not only be the first to get

critical information about a coming terrorist attack but, with the proliferation of private surveillance technologies and personal communications capabilities, they could be empowered with the critical ability to decide what to do with it. Obviously, the national intelligence community has a stake in such decisions. But not surprisingly, the U.S. intelligence community has neither a roadmap for building the kind of domestic alliances that would facilitate such cooperation nor the deep and nuanced understanding of American political culture that makes such a task so difficult for the federal government to implement.[20]

Unfortunately, terrorists who recognize this trend in private sector surveillance and its potential connection to the nation's information infrastructure may use cyberattacks to facilitate their plans. According to James Gosler of Sandia Laboratory, these attacks are becoming increasingly feasible. His argument, in its simplest form, is that the distributed nature of the modern software and computer manufacturing industry makes modern information technologies inherently vulnerable.[21] Aware of both the threat in the private sector and its inherent vulnerability, the U.S. government decided after 9/11 to circumvent established procedures for domestic counterterrorist surveillance to permit rapid sampling of certain domestic communications as a counterintelligence measure.[22] This step at the federal level has proved highly controversial. Less controversial methods for improving domestic collection could involve building alliances with the private sector rather than simply tapping into it.[23]

DATA FUSION AND THE AGE OF TERROR: IMPLICATIONS FOR DEMOCRACY

The prominent role all-source intelligence and advanced technology have in countering terrorism presents special difficulties for democracies. Although the media have recently highlighted issues related to prisoner detention, rendition, and interrogation, these are not the only matters that trouble democracies fighting terrorists. Debates continue among civil libertarians, security officials and private citizens over the more obscure issues of domestic surveillance, data management and privacy. It is hard to promote freedom and liberty as antidotes for terror while at the same time encouraging allied governments to intrude more deeply into their own societies for the purpose of monitoring individuals and capturing fanatics before they act. Unfortunately, this is exactly the course that the US is now forced to take. Balancing security and pre-emption with restraint and freedom is difficult; terrorists likely hope the conundrum will prove paralyzing.

While some commentators have suggested that privacy may be one area where Americans may be willing to cede added power to authorities, others, including this author, have noted that suspicion of excess power in the hands of the federal government runs deep in American political culture. Although the issues prisoners' rights now before the courts are beyond the scope of this paper; these other issues of data fusion, control, and management are not.

The Domestic Context for Intelligence Collection and Data Fusion

Throughout the Cold War, the CIA, FBI, and certain military services were involved in domestic intelligence collection. When they over-reached, they were subjected to new legal constraints. By 1978, when the Foreign Intelligence Surveillance Act (FISA) was passed, the essential framework for domestic spying in the US had been established: on the one hand, the president's constitutional authority for the nation's defense gave him the prerogative to order domestic surveillance; on the other hand, his powers to spy on American citizens and residents were constrained by the requirement that the courts be convinced of these individuals' connections to foreign powers or terrorist causes in each case. It was understood, if not written into law, that information gathered in this secret way, that is, without the normal warrant process, was not to bleed into the criminal justice system to be used against citizens for other purposes—such as to convict them of a crime unrelated to espionage or terror. In this way, what has come to be called the "wall" between intelligence and law enforcement was deliberately and perhaps too impermeably erected.

After 9/11, lawmakers and national security experts criticized this framework as too tight a constraint on domestic intelligence gathering. While the president was secretly reasserting his perceived prerogatives to spy against domestic national security threats, Congress passed the Patriot Act. This act increased the FBI's ability to track and monitor terrorists using communications systems far more elaborate than those available when the original FISA law was passed. In addition, the "wall" between intelligence and law enforcement was torn down in the interests of intelligence sharing between agencies. The president also decided to consolidate within the Department of Homeland Security (DHS), those agencies responsible for border control, emergency response, and domestic security. While eschewing a new domestic intelligence gathering function, DHS began to consolidate databases and to generate related intelligence reports. The president created the Terrorism Threat Integration Center to fuse intelligence from all relevant agencies both inside and outside the formal intelligence community. Following the endorsement of the idea of data fusion centers by the 9/11 Commission, Congress passed legislation creating the National Counter Terrorism Center, the director of which gained authorities over overseas operations as well. Subsequently, its sister center was created under the new Director of National Intelligence to handle intelligence on weapons of mass destruction.

While these changes were under way at the highest levels in Washington, debate has continued on what appears to be a serious gap: Unlike Britain, the U.S. federal government continues to lack an institution specifically charged with conducting true domestic intelligence gathering and forging the kind of domestic alliances for intelligence networking already described. The FBI's expertise remains law enforcement and defensive counterintelligence—both arts involving the use of surveillance for arrests, not for strategic planning and the exploitation of decision advantages. The CIA and FBI—if not the NSA—have also remained

boxed within the 1978 framework and thus prohibited from even thinking about how to develop knowledge on domestic activities. Without a deep domestic intelligence capability and the domestic consensus necessary to institutionalize it, data fusion at the federal level may remain inadequate to the counterterrorism task.[24]

Unwilling to wait for a federal agency to take an aggressive lead, law enforcement officials in cities such as New York, Los Angeles, and Chicago have begun to expand their capabilities to investigate domestic groups; consolidate the data from global, national, and local sources; and thus organize new and improved intelligence systems themselves. Data fusion is becoming a grassroots business. For example, Los Angeles has pioneered the Terrorism Early Warning Group, which fuses intelligence and directs it to first responders.[25] And New York City has gone so far as to establish liaison offices overseas. In the wake of the collapse of a local cable company, Chicago's Mayor Richard Daley bought up its fiber optic network and hooked hundreds of video cameras to it. He has also encouraged private companies to dump the returns from their surveillance cameras onto the network so that, for a fee, crimes could be rapidly reported to the city's police department.

Of course, the establishments wired for commercial security are becoming Chicago's platforms for law enforcement surveillance of criminal and gang-related behavior. The city's operations center has become the hub of a network for surveillance and monitoring in the name of citizen protection against crime and, simultaneously, natural disasters and terrorist attack. Not surprisingly, Chicago's innovation has been replicated in at least 150 other cities to a greater or lesser degree. New York, which reportedly plans a network of 3,000 cameras, is defending its right to archive the video files indefinitely.[26] Baltimore, whose cameras may soon have the ability to "talk," intends to deter crime as much as counter terrorists with its electronic network.[27]

Other first responders are adopting similar methods for different purposes. Hospitals have begun wiring themselves to keep track of the conditions of patients and the scarce medical equipment they may need to ensure efficiency of care. When more than one hospital participates, ambulances can make better decisions about where to transport emergency cases to ensure the swiftest medical care at emergency rooms. A system such as this, or the one in Chicago, could have assisted New Orleans in its efforts to respond to the emergency following Hurricane Katrina. It holds the promise of gathering data swiftly and analyzing it appropriately in the event of a terrorist attack as well.

Although public protests of increases in domestic surveillance at the local level have been light and sporadic, this level of tolerance has not been apparent when federal surveillance has been involved. National attention more readily focuses on federal moves, hesitant though they may be, to increase domestic surveillance. For example, the president's expansion of the Defense Department's Counterintelligence Field Activity (CIFA), including its surveillance activities nationwide, has triggered protests, including at least one congressional intervention.[28] Although CIFA was created to protect military facilities and

personnel worldwide, it has significantly ramped up its domestic operations in recent years for the purpose of fusing intelligence, identifying and assessing threats, and retaining the results in a Pentagon database.

Perhaps even more notorious was the abbreviated effort to link databases at the federal level for similar purposes. In 2003 Adm. John Poindexter spearheaded an effort to link databases at the federal level for the purposes of querying them and drawing inferences about terrorists actions from their contents over time. The project, unfortunately dubbed Total Information Awareness (TIA), had an Orwellian quality that made many Americans' hair stand on end. Among them were a number of legislators who promptly killed the program. Along with it, they killed the only ongoing federally funded research in how to protect the privacy of citizens from advances in "inferencing" capabilities (discussed below), so crucial to anticipating, warning, and managing not just terrorist attacks but natural disasters and outbreaks of disease as well.

For reasons elaborated more fully elsewhere, Americans clearly have a particular distaste for federal government intrusion in their lives.[29] That the citizens of a small town in Vermont wire their streets with surveillance cameras or that Chicago and New York and Baltimore experiment in new law enforcement techniques does not mean that the American public will be willing to accept those kinds of domestic initiatives from the federal government. This attitude holds true even when the nation's security is arguably at risk. Although the relevant laws have been modified in the wake of 9/11, citizens are likely to demand that constitutional protections against unwarranted intrusion by the federal government stay intact even as they willingly cede these rights to commercial firms and local law enforcement.

WHAT IS TO BE DONE?

Britain's successful counterintelligence operation against communist infiltrators during the interwar period involved the use of domestic surveillance, communications intercepts, direction finding involving the military services, and the penetration of a domestic political party. Such an aggressive approach would be firmly resisted in the United States, constrained as it is by the electorate's deeply seated sense of domestic privacy and individual prerogatives. Yet without successful efforts to bring together all-source intelligence on domestic threats, a repeat of tragedy on the scale of 9/11 could bring the kind of domestic overreaction that leads to vigilantism and the undermining of the very constitutional protections that national security measures are meant to protect. So what can be done to balance the need for data collection and fusion with civil liberties?

Challenging as the technological political landscape seems, it also presents opportunities for domestic counterterrorist operations, provided secret breaching of democratically developed laws does not trigger public blowback. Terrorists have gained an advantage in operating within democracies because they have found

ways to use technological innovations, such as the Internet and commercially available programs for communicating, hiding, and ferreting out new recruits. This penetration of liberal societies through the hijacking of the technologies they excel at creating is crafty. After all, Americans entrepreneurs rapidly employ their best commercial innovations in critical infrastructure, protecting them as national assets even as adversaries exploit them.

But technology is, by its nature, neutral. It is also constantly changing. The American public has proved itself both adaptable and tolerant of efforts to fuse intelligence for the purposes of interdiction, at least when done at the local level. The issue is whether those officials countering terrorism can be quicker and more innovative than the terrorists in recognizing what must be done in binding innovation to mission and whether citizens and officials at the local, state, and federal levels can find ways to embrace such innovation without doing violence to civil liberties.

Pursuing Total Information Awareness?

Although no one would suggest that American citizens should embrace an Orwellian world in which the federal government monitors their every move, most Americans probably do understand and even value society's ability to remember them when their lives and livelihoods are at stake. Insurers and pharmacists keep track of medical records; credit card companies and banks track credit histories so that people can borrow money to buy homes or send their kids to college.

What is at issue is the government's ability to access and combine these pools of data to uncover patterns of activity. Though such pooling might lower the risks to society, it could have unfortunate consequences for individuals in specific instances: a personal medical history falling into the hands of prospective employers; fallacious patterns that seem to implicate an innocent person in the activities of a gang; or the confusion of a name and profile of a suspected terrorist with that of a law-abiding citizen. At the same time, failure to establish such patterns may allow terrorists free rein in a society increasingly wired for their purposes.

Two avenues are open for addressing this dilemma. First, research institutions can delve more deeply into the question of data mining and analysis and educate the public about their results. Public understanding of the uses and limits of government held databases is currently minimal. And although institutions such as the Center for Strategic and International Studies have begun important initiatives to raise public awareness of the true nature of the data-mining question, much more needs to be done.[30]

Second, the U.S. government can more proactively align itself with domestic initiatives to fuse data for crisis management in the private sector and for local law enforcement purposes. In return for encouraging and even subsidizing those initiatives that have found support among local citizenry, the federal government

could share federally researched techniques and standards for information processing and hand-off, while negotiating protocols for ensuring the threshold for federal access is appropriately restrictive.

Data Mining and Data Analysis: Thinking Ahead

An expert with the Center for Strategic and International Studies, Mary De Rosa, has conducted a carefully researched study of the data fusion and management problem confronting counterterrorism analysts.[31] Data mining has proved a particularly nettlesome area for domestic intelligence. In her published report, De Rosa makes important headway by drawing clear distinctions between data mining and data analysis. The former is a process that "uses algorithms to discover predictive patterns in data sets"; the latter "applies models to data to predict behavior, assess risk, determine associations or do other types of analysis."[32] Although both techniques simply exploit data that are already accessible, they also create new knowledge from these data faster and more accurately than human analysts can. Specifically, these techniques can help with the accurate attribution of records to individual people; establish connections between people, places, and things; and infer from existing data, using patterns of past illicit activities associated with known terrorist groups, the probable development of sleeper cells involving individuals with no known criminal records. What many of these systems do far less efficiently is discern data that no longer require archiving. The absence of such self-laundering systems means that inappropriate associations among data sets may linger. This means that innocent civilians may only notice that they have a problem when pulled out of lines at airports or encountering difficulties renewing their driver's licenses.

As these techniques are being developed in the private sector by commercial firms interested in increasing profits by understanding markets, the general public is intermittently outraged, perplexed, or delighted with the impact of these developments on their personal transactions. Most private citizens remain largely unaware of business and government investment in both data mining techniques and technologies designed to moderate their deleterious effects on privacy. De Rosa includes in her list of such advances anonymizing, auditing, and "permissioning" technologies. Investors are funding anonymizing techniques to allow data on individuals to be processed without using names. The second type of technology, auditing, allows those working on newly enabled data-processing techniques to be held accountable for their actions. Permissioning would ensure that rules established for handling data are fully respected.

Unfortunately, De Rosa concludes that even if the problems of inappropriate associations among data—that is, the problem of false positives—can be overcome, government mechanisms remain inadequate for controlling the use of the results. Among the issues that still need to be addressed are those related to mission creep, or the tendency to do more with information than the public has agreed to tolerate.

Enlisting the Private Sector: Smart Buildings?

It is not much of a stretch, given advances in data processing and the steps already taken in Chicago and New York, to see that in the event of a terrorist attack, the federal government would have potentially wide-ranging interest in information being generated in localities. Doctors, hospitals, and private surveillance cameras could become the new collectors in a nationwide intelligence effort to learn what the terrorists have done, where they have gone, and where they might attack next.

If such a system were developed and automated, the advantages would flow to both local crisis managers and the federal government. Doctors and hospitals could concentrate on care of the victims while an impersonal data hand-off of symptoms and geographic distribution could be provided to authorities responsible for determining if terrorists and biological weapons were involved. This would enable a quick, nationwide response. For example, if San Francisco, Houston, and Seattle were also equipped, the federal government would have instantaneous information from across the country should simultaneous attacks—the hallmark of terrorist groups such as Al Qaeda—occur. The capacity to learn about attacks and their nature early on would make the difference in the federal government's capacity to respond to such events.

Hospitals are not the only wired domains that might be lashed to such a nationwide 911 system. Indeed, technological innovations are moving swiftly toward a city landscape likely to differ greatly from the cities of today. Nanotechnology promises to offer micro-energy systems embedded in the skins of buildings that use solar power as energy for wireless sensing, lighting, and maintenance devices. Buildings already equipped with fiber optic cables of the kind laced through Chicago may soon have the ability to sense and control not only environmental conditions within them but the air quality and environmental conditions outside. In the event of disasters, these buildings may someday have the "sense" to seal themselves, control and clean air flows, and monitor the health, location, and well-being of their residents while sending this information to first responders and, if necessary, the federal government.

After all, the technologies that Chicago, New York, and now Baltimore are discovering turn on automated data analysis: "inferencing engines" that fuse sensor data from multiple inputs. These inferencing capabilities help assess not only what is happening at the moment but also what might be coming. In other words, by fusing lots of data simultaneously—far more data than a human analyst can cope with in a normal day—and applying sophisticated models, computers are able not just to see what has already happened but warn of coming events. From a counterterrorism standpoint, far better than hunkering down in buildings that protect their occupants from the effects of biological terrorism would be a system that sorts tremendous amounts of data and anticipates the attackers before they are able to act. This kind of data fusion for counterterrorism would permit consequence management as well as interdiction and protective actions prior to attack.

At the point where technology turns buildings into allies, the need to evacuate cities in the face of many kinds of disasters may pass. The trick, of course, would be to ensure that technology stays friendly and in the right hands. If technology is moving in this direction, and indications are that it is, the federal government needs to anticipate the wired society that is emerging and work to ensure that the protocols, access, and management of this information stays within the scope of tolerance for Americans not only protective of their families and well-being, but also of their freedoms and privacy as well. Such a legislative package would set the bounds for federal surveillance of domestic threats and the proper procedures for handing off information collected at local levels for civilian purposes, to the federal level in times of crisis or elevated threat.

CONCLUSION

In recognition of the rapid tempo of decision making so necessary for interdiction of terrorists—especially those possibly equipped with weapons of mass destruction—the intelligence community has organized centers for counterterrorism and nonproliferation that marry analysts with operators and technology specialists so that they can more rapidly fuse intelligence data, analyze it, and act. The military has employed a form of this approach since the first Persian Gulf War with its creation of National Intelligence Support Teams and now Joint Intelligence Operations Centers that fuse all collected data from tactical and national level sensors to support commanders' operations in the field.

What the federal government has been slower to do is to reach out to the private sector in support of initiatives such as those in Chicago and New York for the purpose of negotiating frameworks or protocols for the hand-off of information to the federal government under certain specified conditions.[33] Arguably, the best time to negotiate these solutions is now, before the next terrorist attack takes place and a spasm of reaction leads to measures not nearly as well thought out as the American polity deserves. At the same time, initial efforts to manage just the federally available information for such purposes has met with stunning political resistance from a poorly informed public. Burned once, the political will to bridge the Washington–locality divide may be hard to muster in the future.

To take these necessary steps, the United States needs to muster the will for a public debate on privacy—not seek to avoid it as a bothersome drag on the mission of law enforcement and counterterrorism experts. The need is now urgent. Between the great world wars of the last century, Britain succeeded in protecting its polity from the threats posed by an international network intent on penetrating and corrupting it. It did so by employing all-source data fusion—to include data from domestic sources still beyond the scope of what federal intelligence authorities are permitted under U.S. law. A great American debate awaits over the extent to which the federal government can ally with state and local governments and private industry to manage the new, secure information infrastructure that is

already emerging to enable domestic intelligence authorities to do their job, within the law, as Americans expect them to.

NOTES

1. Nigel West, *MASK: MI-5's Penetration of the Communist Party of Great Britain* (London: Routledge, Taylor and Francis, 2005). This description of MASK and its accomplishments are derived from West's excellent work on the subject.

2. Ibid.

3. This argument on the nature of intelligence is expanded in my draft article, "Smart Realism: A Theory of Intelligence in International Politics," April 2006.

4. Surprise is properly understood as the extension of a counterintelligence effort because it involves learning how the opponent thinks and acts and then making a strategic or tactical move designed to exploit weaknesses in that decision-making process. Surprise can be achieved by simply getting inside the decision loop of the adversary: Even if intelligence provides warning, the victim cannot turn warning into effective action in time to stop his losses.

5. For more on the similarities of strategic decision making among gangs, mobs, and nation-states, see Thomas C, Schelling, *The Strategy of Conflict* (London: Oxford University Press, 1968), especially pp. 12–13.

6. I owe the insight on the connection between intensity of competition and the need for secrecy to enlightening discussions of intelligence theory with my friend and colleague Michael Warner, CIA historian, over the winter of 2005–2006. Getting any of this wrong is, of course, my responsibility, not his.

7. Most literature on open-source intelligence focuses on the role cheap, unclassified information can play in limiting the burden on precious, classified collection systems. But this leaves the comparative advantage for democracies partially unexploited and a fixation on the primacy of secrets intact. Speed may be more important than data source when stopping terrorists in our midst—and sifting huge quantities of data takes time. Intelligence managers should consider how classified information could be exploited to help target unclassified sources and databases to get the jump on an adversary. Creativity—and sloughing off old prejudices—is needed in thinking about the role of open sources in intelligence.

8. This last form of collection is known as measurement and signatures intelligence, or MASINT.

9. The importance of all-source collection for these purposes is discussed in Steve Coll, *Ghost Wars* (New York: Penguin Press, 2004), pp. 492–93.

10. The concept of boosting is discussed in greater detail in Jennifer E. Sims, "Smart Realism: A Theory of Intelligence in International Politics," paper presented to the Georgetown Intelligence Salon, April 2006. For more on this concept, see Michael Herman, *Intelligence Power in Peace and War* (London: Cambridge University Press, 1996), pp. 65–66.

11. This is a widely known technique for locating radio signals. In fact, amateurs engage in DF competitions under the sponsorship of the International Amateur Radio Union. For more on the term *DF*, see http://en.wikipedia.org/wiki/direction_finding.

12. For more on the Gestapo's efforts against Stalin's spies in Europe, including the use of DF against HUMINT cells, see V. E. Tarrant, *The Red Orchestra* (London: Wiley, 1996).

13. Michael Herman writes: "Espionage can also help other collection activities. Human sources are sometimes needed to plant bugging devices. Cipher-breaking has often been assisted by obtaining copies of codes and cipher material through human sources. Acquiring agents with this kind of cryptographic access was always one of the KGB's highest priorities." Herman, *Intelligence Power*, pp. 65–66.

14. See J. C. Masterman, *The Double-Cross System: The Incredible True Story of How Nazi Spies Were Turned into Double Agents* (Guilford, CT: Lyons Press, 2000). Also see Anthony Cave Brown, *Bodyguard of Lies* (New York: Harper & Row, 1975).

15. For an excellent history of the dangers of weak counterintelligence in an interlaced collection system, see Leo Marks, *Between Silk and Cyanide: A Codemaker's War* (New York: Touchstone, 1998).

16. John Arquilla and David Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001).

17. See Stephen Budiansky, *Queen Elizabeth I, Sir Francis Walsingham, and the Birth of Modern Espionage* (New York: Penguin, 2005).

18. Jeffrey T. Richelson, *A Century of Spies: Intelligence in the Twentieth Century* (New York: Oxford University Press, 1995), pp. 27–30.

19. Unfortunately, law-abiding citizens sometimes suffered discrimination, undeserved punishment, and retribution in the process.

20. The point about local empowerment may have been dramatically illustrated by the decisions of individual Finns to use their Nokia cell phones during the immediate aftermath of the 2004 tsunami in the Indian Ocean. Empowered by their individual communications devices, which offered a direct link back to Helsinki, Finnish citizens were able to provide critical information for their government's decision-making process. (Based on author's informal interviews with officials and Nokia personnel in Finland during June 2005.) The notion that U.S. intelligence has poor appreciation of domestic cultural issues related to its profession should not be controversial. After all, intelligence systems have long been suspect elements of democracies and, in any case, have focused their attentions against adversaries, not on deepening knowledge of the societies in which they operate. This may be changing now. For lengthier discussion of the American cultural context for intelligence, see Jennifer E. Sims, "Understanding Ourselves," in *Transforming US Intelligence,* eds. Jennifer E. Sims and Burton Gerber (Washington DC: Georgetown University Press, 2005).

21. James Gosler, "The Digital Dimension," in *Transforming US Intelligence,* eds. Jennifer E. Sims and Burton Gerber (Washington DC: Georgetown University Press, 2005), pp. 96–114.

22. These procedures were established in 1978 when Congress passed the Foreign Intelligence Surveillance Act (FISA). This act limits the president's authority to conduct wiretapping for national security purposes by requiring federal intelligence and law enforcement authorities to get warrants for such surveillance from a secret court. Some legal experts argue that the act is unconstitutional because it involved one branch of government (Congress) circumscribing the constitutional authorities of another branch (the president). In any case, many observers noted that FISA had been widely regarded as settled law and that challenges to it should have been publicly debated in the context of,

for example, the USA-PATRIOT Act, which was meant to amend previous domestic surveillance laws to post-9/11 circumstances. Others argued that such open debate would have revealed too much of our counterintelligence capabilities to the adversary.

23. For more on the idea of domestic alliances for intelligence purposes, see Henry C. Crumpton, "Intelligence and Homeland Defense," in *Transforming US Intelligence,* eds. Jennifer E. Sims and Burton Gerber (Washington DC: Georgetown University Press, 2005).

24. Ibid.

25. John P. Sullivan, "Terrorism Early Warning Group and Co-Production of Counterterrorism Intelligence," paper presented to the International Studies Association conference in San Diego, March 21–25, 2006. Also presented to the Canadian Association for Security and Intelligence Studies, 20th Anniversary International Conference, Montreal, Quebec, Canada, Panel 5, October 21, 2005.

26. Constituent Works, "Court Hears NYPD Surveillance Camera Case," March 27, 2006, available at http://www.officeoutlook.com/news/security/1147.htm (accessed April 7, 2006).

27. Associated Press, "Baltimore's Latest Crime Tool Is the Talking Camera," available at http://www.policeone.com/police-products/investigation/video-surveillance/articles/121178 (accessed April 7, 2006).

28. Walter Pincus, "Pentagon Will Review Database on U.S. Citizens: Protests Among Acts Labeled 'Suspicious,' " Washingtonpost.com, December 15, 2005, p. A01. Indeed, Senator Feinstein wrote a letter on January 10, 2006, to Secretary of Defense Rumsfeld requesting additional information on CIFA practices, including the retention of TALON reports on the activities of private citizens engaged in activities protected under the First Amendment.

29. The history of American skepticism of domestic surveillance is admirably covered by Christopher Andrew in his excellent history, *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush* (New York: HarperCollins, 1996).

30. Mary De Rosa, *Data Mining and Data Analysis for Counterterrorism* (Washington DC: Center for Peace and Security Studies, March 2004).

31. Ibid., p. v.

32. Ibid.

33. The Department of Homeland Security has provided some funding for these initiatives. However the development of privacy protocols, called "appliances" under the now-defunct TIA initiative, has languished. For more information, see "Chicago Moving to 'Smart' Surveillance Cameras," available at http://www.policeone.com/products.

9

WOMEN IN RELIGIOUS TERRORIST ORGANIZATIONS

A Comparative Analysis

KATHARINA VON KNOP

WOMEN HAVE BEEN ACTIVE IN VARIOUS TERRORIST groups throughout history. All of these women undermine the idea of who and what a terrorist is. What is generally not realized is the extent to which women are involved in terrorism.[1] The purpose of this chapter is to explore and analyze the multifaceted roles of women in religious terrorist organizations. My argument is that the role of women perceived by the world audience is one of a suicide bomber. However, the role of an ideological supporter and operational facilitator is even more important for the maintenance of operational capabilities, ideological motivation, and survival of a terrorist organization.

To verify these arguments, the chapter is divided in three parts. The first will look at what motivates women to participate in a terrorist organizations and what motivates a terrorist group to use women for its purposes. The second part will analyze the role of women in Palestinian terrorist organizations. Finally, the third part sheds light on the women of the global Salafi Jihad. For that purpose the female attacks of the global Salafi Jihad will be analyzed.

The findings of this chapter with regard to the involvement of women in Palestinian terrorist organizations and the Al Qaeda movement will bring us to conclude that women play a growing and essential role in these groups.

INTRODUCTION

The concept of terrorism, particularly against soft targets, is shocking enough to most liberal Western audiences; however, the use of female attackers exacerbates the already potent psychological effect of suicide terrorism. Women's

involvement in terrorist organizations is long and established. They have been active in various terrorist groups in various positions throughout history. One of the most famous instances of modern international terrorism, and the first that received global media coverage, was led by a Palestinian women, Leila Khaled. This senior Popular Front for the Liberation of Palestine (PFLP) operative was involved in the hijacking of an Israeli plane in 1969 and a second one in 1970.[2] There have been other famous female terrorists, such as Ulrike Meinhof from the Red Army Faction and Patty Hearst from the Symbionese Liberation Army (SLA). Cases such as these, in which women act as leaders of terrorist organizations, are rare, but they do exist. In Germany, the Red Army Faction and the Red Brigades had women leaders and cofounders. Khaled is a member in the Leadership Council of the PFLP.[3] The current chief of staff of the Basque separatist organization Euskadi Ta Askatasuna (ETA) is reportedly a woman. The Japanese Red Army has also had women leaders. In various Latin American organizations, such as Peru's Sendero Luminoso (SL), women accounted for as much as 20 percent of the fighting force.

Every terrorist group in Western Europe has used women combatants. Other organizations that are currently composed of large numbers of women include the Tamil Tigers of Tamil Elam (LTTE) and the Fuerzas Armadas Revolucionarias in Colombia (FARC) among others. The first "successful" female suicide bomber was a 17-year-old Lebanese girl named Sana Mahaydali, who was known as the "the Bride of the South." In 1985, she was dispatched by the PPS, a pro-Syrian Lebanese organization, to blow herself up near some vehicles carrying Israeli soldiers in Lebanon. "This paved the way for several other Lebanese women acting on behalf of other terrorist organisations. From Lebanon, the use of female suicide bombers spread to other countries and within few years was adopted by the LTTE and the Kurdish PKK."[4] The women of the LTTE are responsible for one-third of all suicide bombings in Sri Lanka, whereas the female PKK (Kurdish Workers Party) members have carried out two-thirds of that group's suicide bombings. What these groups have in common, however, is that they are or were leftist or nationalist-separatist oriented.

During the past few years we have seen many changes occur within religiousterrorist organizations. One of the most surprising developments has been the way suicide terrorism by religious groups has opened the stage for entry of female combatants, who are increasingly involved in what was once an exclusively male-dominated area.

Over the past few years, women have played a central role in the Chechen campaign of suicide bombings directed against Russia, and since 2002 female suicide bombers have become an established force in Palestinian terrorist organizations. In April 2003, as a predictable surprise, the first female suicide bombers blew up their car at a coalition checkpoint in Iraq. One of the two women was pregnant. Al Qaeda claimed responsibility for the suicide attack carried out by a woman on September 28, 2005, in Talafa in northern Iraq against a U.S. military recruitment center, with the statement: "A blessed sister . . . carried out a heroic

attack defending her faith. . . . May God accept our sister among the martyrs."[5] Even though the use of female suicide bombers in Iraq is still a relatively new trend, women will likely play a wider role in operations where terrorist groups mobilize an entire population.

For terrorist organizations as rational actors there are a number of operational advantages in the use of women as suicide bombers, supporters, and facilitators, because women undermine the idea of who and what a terrorist is. The intuitive assumptions presume that terrorists and terrorism is a man's domain. Most people still believe that women would not kill in such a barbaric and indiscriminate way that targets innocent people. This is why there is usually a public outcry of horror against women terrorists.

The function of women in religious terrorist groups and movements is multifaceted. The role that the world audience perceives is that of a suicide bomber; however, the role of an ideological supporter and operational facilitator is even more important for the maintenance of operational capabilities and ideological motivation. In sum, even when women are invisible to the world audience, they play an essential role in the short- and long-term survival of terrorist organizations.

THE MOTIVES OF THE WOMEN AND THE ORGANIZATION

Since 2002, female suicide attacks on behalf of religious terrorist organizations has been on the rise and is expected to increase in the future.[6] Though the personal motivations of female terrorists differ from the organizational motives for recruiting them, the two sides converge to produce an increased number of female terrorists. In these groups, the use of women in terrorist attacks is rare but not a new issue. Some of the most shocking recent incidents of female suicide terrorism have occurred during the current Israeli-Palestinian conflict. Suicide bombing, particularly during the present Intifada, has become one of the dominant features of the asymmetric campaign being waged against Israel by the Palestinian terrorists.

Female terrorism is increasing because women are motivated to engage in political violence and organizations are facing stronger incentives to recruit female operatives. To understand why female terrorism is on the rise, the societal, individual, and organizational motives must be explored. At this point, it should be mentioned that throughout history, women have played a relatively minor role in these terrorist groups.[7]

Media reporting has often suggested that most female suicide bombers, like their male counterparts, go eagerly to their deaths fueled by an unshakeable fervor; but the truth may be more complex. Although there are no concrete figures concerning the extent of women's current involvement, many commentators have observed that female participation in terrorism has significantly increased since 1976.[8]

The use of female suicide bombers could be found in many different kinds of terrorist organizations, but female terrorists share more then the use of terrorism as a fighting strategy. Female suicide bombings occur in the patriarchal societies from which these women originate and are the result of the deeply rooted values separating the women's roles from those of the men. Female terrorists are motivated by many of the same reasons men are, but the gender-based oppression they face creates additional motivation. Barbara Victor states that "the real reasons that motivate women, as opposed to the rational that creates male suicide bombers, are subtle and indicative of the second-class status of women in that part of the world."[9] All of the societies that have witnessed female suicide bombings are those where women are restricted to the private sphere. While women stay at home, men's tasks are conducted in the outer world. In traditional societies, gender defines acceptable activities and assigns particular roles to both men and women. Men hold a position of power and dominance, giving them full reign of the public domain. Women are relegated to the private sphere and are constrained in all areas of life. Rhiannon Talbot argues that women terrorists reject female roles and adopt the traditional male role of violent activity.[10] This violence occurs in the public realm from which women are otherwise excluded.[11] Female terrorists are thus able to pursue opportunities other than the limited ones available in traditional societies. This suggests that the existence of female subordination is linked to female participation in terrorism. As agents of violence, women are no longer defined according to their gender roles.

The PKK in Turkey also offered women an alternative to traditional gender roles and provided them access to the public domain. The Kurdish terrorist organization was the only structure that offered women a choice other than the traditional one of wife and mother. The group offered women the opportunity to be upgraded to the status of warrior. Within the organization, women would not be defined as a man's subordinate anymore, nor simply as wives or mothers.[12]

I argue that the scope of women's power interests are shaped by the society they live in. This scope in patriarchal society is normally the family. Encouraging and supporting the male relatives to participate in a terrorist organization gives women power and access to the public realm. Carrying out attacks allows women to fulfill traditional male duties: to carry out an political act and have the chance to be honored by the society they are living in. Talbot argues that this development is an act of female liberation and emancipation in these male-dominated societies. For instance, Yoram Schweitzer states: "The willingness of fundamentalist Islamic organisations to make use of women in their suicide operations contradicts the principle of religion as well as traditional social norms that preclude the involvement of women in 'masculine' activities that require close contact with men to whom they are not married."[13] I reject the argument that female suicide bombers in Islamist societies are acts of female liberation, because these women are recruited by men who are members of the terrorist organization. The explosives were provided by men, and the women were instructed by men on how to use them. This behavior is misinterpreted as female liberation or emancipation.

Being a suicide bomber is a learned behavior that results from the absence of other role models. Especially in Palestinian society, the only way to become a female hero is by carrying out a suicide attack.

However, in effect, being a suicide bomber amounts to total submission under a male-dominated terrorist organization. As mentioned, patriarchal societies, especially those that host terrorist groups, only offer two role models for women. The first is to be the mother of as many as children as possible, and the second is to be a suicide bomber. The only way to be honored by the society is to carry out a suicide attack in support of the ideology and the terrorist organization. The ideological goal and the struggle have priority over the battle of the sexes. These women adopt the masculine concept of Jihad for political reasons. Khaled brings it to the point: "So if this society doesn't mobilize all of its energy to face down the enemy, it can't achieve victory. A Palestinian woman is a Palestinian as well. As such, she has the same goals as the rest of our people."[14] This acceptance goes so far that religious leaders have found interpretations of the Koran to justify female suicide bombers and the supporting role of the women in this male-dominated ideology.

Attempts have been made to profile female suicide bombers in the hope of finding common threads in their backgrounds and motivations. However, it is very difficult to profile female suicide bombers or female facilitators and supporters because they come from very diverse educational, religious, social, and personal backgrounds.

Many women choose to join a terrorist organization to seek vengeance. Terrorism continues to be a male-dominated activity, and it is men who suffer the majority of casualties from counterterrorism, failed missions, and successful suicide bombing operations.[15] Faced with the loss of male family members, women are motivated to take up arms. This phenomenon is observable where women's participation in terrorism begins at a later stage than men's. In Chechnya, female terrorists are called Black Widows, and they are "prepared to kill and to die to avenge the deaths of fathers, husbands, brothers and sons at the hands of Russian troops in the current war or the one in the 1990s."[16] These female bombers are in part a direct reaction to Russian military tactics. The human rights group Memorial adds that another contributing factor is the routine rape of the Chechen women by the Russian soldiers. Although female participation was negligible throughout the 1990s, the Chechen groups suffered severe male casualties, and female suicide bombers have now become more common.[17] Women's active participation began in October 2002, and since that time Black Widows have been blamed for the deaths of over 200 people in nine attacks. These women are driven to terrorism by a desire to regain their personal or family honor.

As previously mentioned, women in traditional societies are governed by a strict set of social, cultural, and religious rules. In Palestine, for example, these rules prescribe the separation of men and women, and require women to be physically covered and chaperoned by a male family member when in public. If a woman breaks these rules, she is ostracized by society and brings shame on

herself and her family. As a result of this marginalization, women may seek refuge in a terrorist organization. These groups offer a double benefit to these women by accepting them when they no longer have options in mainstream society and by allowing them to regain their honor by committing a terrorist act. By participating in armed struggle, these women are able to gain the dignity in death that they lost in life.

In Sri Lanka, terrorism is often seen as a viable option for Tamil women who are survivors of sexual violence. Following a rape, Tamil women are considered damaged goods, and social customs prevent them from getting married or bearing children.[18] The shame brought on by sexual violation is thus magnified by the humiliation of being unable to fulfill childbearing duties and desires. Many of these women join the LTTE because, unlike mainstream society, it does not condemn or marginalize women who have been raped.[19] Societal expectations of procreation are so fierce that families of rape survivors have been known to actively encourage these women to join the LTTE.[20] Tamil culture encourages women to advance their children's interests at the expense of their own welfare, but female self-sacrifice for her community by engaging in terrorism can serve as an acceptable substitute.[21] Their participation compensates for their inability to give birth to future generations and restores their personal and familial dignity.

Even today, when women are playing an increasing role in violent organizations, they still represent a minority of the total membership. To understand the low scale and the rise of female terrorism, organizational motives for recruiting women must be explored. Women may want to become actively engaged in the conflict, but the evolution of the role of women from supportive to active is initiated at the organizational level. There is a great disparity between what motivates women to join a terrorist group and what encourages a group to recruit women.[22] Regardless of a woman's individual motives, terrorist groups are rational actors acting on the basis of cost-benefit calculation. The use of terrorist violence is part of a political strategy and represents "a willful choice made by an organisation for political and strategic reasons."[23]

Changes in targets, perpetrators, and tactics can be understood under this framework. The use of female operatives in a male-dominated activity represents a tactical change by terrorist organizations. These groups "tend to adapt to high levels of external pressure by altering their techniques and targets."[24] Women provide many benefits to terrorist groups, and organizations are increasingly recruiting them as a strategic choice. The use of women provides a new media dimension, which the terrorist group intends for the media to interpret as an indication of a worsening situation. Media images of women terrorists serve as powerful propaganda tools. As we all know, suicide bombers provide a low-cost, low-technology, low-risk weapon that maximizes target destruction and instils fear. Women are even more effective at this with their increased accessibility and media shock value. Female terrorists tend to garner more media attention than men because the "thought of those who bring forth life actually destroying it, is disturbing."[25] The idea of women acting as agents of violence runs completely

counter to expectations of femininity; images of female terrorists thus attract widespread publicity and disseminate the organization's message to a wider audience. Terrorism is a form of psychological warfare, and in this context, the use of women as terrorist operatives is simply a means of upping the ante.[26]

If organizations believe that increased female participation is advantageous, they are likely to encourage this participation in any way possible. Religious justifications, for example, have been manipulated to facilitate more women terrorists. Though the Islamic religious establishment has long opposed and actively condemned women's participation in violent struggles, it has dramatically changed its position more recently. Having seen the positive results and strategic benefits of allowing women's participation in terrorism, the religious establishment has gone so far as to provide an ex post facto justification for women's involvement in terror.

Finally, female terrorists have a greater capacity for mobilizing support than their male colleagues.[27] Female terrorists provide strong role models for other women who may then seek to emulate their heroine's actions. Female terrorism also increases male recruitment because men can be shamed into joining when women appear to be usurping their dominant role in conflict.[28] For example, following the first female Palestinian suicide attack in January 2002, the Egyptian Islamist weekly newspaper *Al-Sha'ab* taunted, "It is a woman, a woman, a woman who is a source of pride for the women of this nation and a source of honour that shames the submissive men with a shame that cannot be washed away except by blood."[29] In order to mobilise both men and women, female members are important for maintaining the recruitment mechanism of terrorist organisations.

Though terrorist organizations seek to achieve many goals, their primary objective is survival. Women are often recruited when membership is dwindling and there is a pressing need for more fighters to continue the struggle, for example, in protracted conflicts or following severe losses of male members. In Sri Lanka, for example, women have been actively involved in the LTTE since 1986, but the number of female fighters significantly increased after 1990. In June of that year, the LTTE suffered significant losses in the battle at Elephant Pass, and women were called to action to replace the losses.[30] The long-term survival of a terrorist group is often dependent on female participation to fill the ranks, either through direct involvement or by persuading men to join.

Female suicide bombers therefore provide many considerable advantages for terrorist organizations. First, they provide a tactical advantage: stealthier attack, an element of surprise, hesitancy to search women, and the stereotype of women as being nonviolent. Second, including women as suicide bombers increases the number of combatants. Third, this would increase the publicity of an attack and, finally, the psychological effect would be much higher.

Today, female participation in terrorist organizations is in its formative stages. But this development poses a challenge to national security services, because the participation of women in suicide bombings broadens the profile of who is considered to be a terrorist. Most counterterrorism measures focus on

men. Women are still less suspicious among security staff around a guarded target; to preserve a woman's decency, security staff is generally more reluctant to subject her to as thorough a body search as they would a man. Some groups, such as the LTTE or the PKK, have allowed women to participate at every level of group activity. It could be just a question of time until we see a similar development in other terrorist organizations.

PALESTINIAN FEMALE TERRORISM

Even though it is still an exception when women carry out attacks in the name of Al Qaeda, we are able to observe some noteworthy developments in other Islamist-based terrorist groups like Hamas and Tanzim.

The women involved in Palestinian terrorism support their male relatives in following the ideology of the terrorist groups; they facilitate operations on a preparatory level, and they also carry out suicide attacks themselves. Looking at the suicide attacks carried out by Palestinian women, we can clearly see how the phenomenon has grown, both in scope and in the type of attack. In 2004, fifty-nine women have attempted attacks against Israelis.[31]

It is hard for many Westerners to understand how Palestinian mothers could sacrifice or push their children to die for "the cause." Creating a supportive social environment for terrorists has been a critical factor in the Palestinian Authority's (PA) successful promotion of suicide terrorism. To this end, PA policy has been to honor terrorists as *shahids* (martyrs for Allah), and to teach Palestinian mothers to celebrate when their children die as terrorist shahids.[32]

On several occasions, these mothers have been shown on television rejoicing over the death of their children. For instance, on November 17, 2004, a mother of two suicide attackers said in an interview with PA TV: "No. We do not encourage our sons to die. We encourage them to shahada [death for Allah] for the homeland, for Allah. We don't say to the mothers of the shahids, 'We come to comfort you,' rather, 'We come to bless you on your son's wedding, on your son's shahada. Congratulations to you on the shahada.' For us, the mourning is a wedding. We give out drinks, we give out sweets. Praise to Allah, our mourning is a wedding."[33]

Nahed Habiballah argues that there are several factors that complicate the role of these mothers.[34] Most of them admit that they venture out to the streets looking for their children and tried several times to prevent them from going to confrontation areas where the Israeli Defense Force is present. Patriotism hinders their effort, however, and they are caught between two extremes: on the one hand, they want to protect their children and prevent their deaths, but, on the other hand, the Intifada is a quest for freedom, and loss of life is possible in such situations. What complicates things even more is the fact that martyrdom has become ingrained in the Palestinian culture over the past two decades, and women have found themselves trapped in a society that provides support for mothers of martyrs while demanding that these mothers become public figures of steadfastness and

pride. These mothers are unable to recover from their losses, because they are not allowed to grieve for their children. In Islam, martyrs are considered alive in heaven, and pious Muslims should not grieve the loss because, unlike the dead, these martyrs obtain the ultimate prize: being in heaven in the company of God and his prophets.

Al-Khansaa is considered the archetypal mother of shahids, a woman glorified by Palestinians for encouraging her sons to kill and die for Allah and rejoicing when they achieved their shahada deaths.[35] Promoting the Al-Khansaa ideal for Palestinians is a very powerful message for Muslims. This portrayal of the ideal Palestinian woman as one who willingly sacrifices her sons as shahids continues to represent official PA ideology. From a very young age, Palestinian girls are taught to adopt Al-Khansaa as a role model with her message of celebrating death in combat, which in contemporary Palestinian society includes death while committing acts of terror. A music video for children, broadcast hundreds of times over three years on PA TV, included the farewell letter of a child shahid, including the words: "Mother, don't cry for me, be joyous over my blood."

Here an additional point needs to be made: Palestinians have made their own cultural set of rules that markedly prescribe gender roles. These rules dictate the separation of the sexes and confine women to the private space of their homes. Their role as fertile mothers and reproducers of the nation marks their utility in the parameter of the conflict as a demographic war. The nationalistic discourse defines a Palestinian woman in terms of her reproductive capacity, thereby making her sexuality and fertility a patriotic and explicitly political issue. Their maternal sacrifice is a supreme political act that is translated into respect and prominent community stature.

The ideology becomes the tranquilizer: the assurance that their children did not die in vain. They died for their country and their ideology, and it is comforting for the mothers who struggle with the pain, loss, and the guilt of not being able to do more to protect their children. It seems that it is easier for mothers who have well-rooted faith to accept the fate that God has chosen for their children. According to the ideology, these mothers should be proud of their children because God chooses the purest people to be martyrs, as they are the ones who are privileged and worthy of his company.

The current trend in the use of Palestinian women as suicide bombers began in earnest in 2002. Wafa Idris, a 27-year-old Palestinian woman from the Al-Am'ari refugee camp near Ramallah, became the first female Palestinian suicide bomber on January 27, 2002, killing an Israeli civilian and wounding approximately 140 others. The military wing of Fatah, the Al-Aqsa Brigades, took responsibility for the attack three days later. This was the first female suicide attack in the Palestinian scene of the second Intifada. Until then, women were generally only employed to support and facilitate suicide operations. The ultimate honor of martyrdom was no longer reserved exclusively for men but had expanded to include women.

Several reasons for this development can be identified. During the current Intifada, as Israel's security forces enhanced their defensive measures against

terrorist attacks, Palestinian militant groups were forced to adapt their tactics, and despite cultural and religious taboos, they began to make increasing use of female recruits. However, a decision to use women in suicide terrorism required clerical sanction, and the tactic was not universally accepted by Islamic militant groups. Indeed, the willingness by some groups to allow women to engage in such activities prompted furious theological debate among radical Muslim clerics. Using women as suicide bombers poses conflict with some leaders's fundamental religious beliefs, while serving a tactical need for a stealthier weapon. In January 2002, Shaykh Ahmed Yassin, the spiritual leader of Hamas, "categorically renounced the use of women as suicide bombers."[36] In March 2002, after the second Fatah bombing, he reported that "Hamas was far from enthusiastic about the inclusion of women in warfare, for reasons of modesty."[37] That position dramatically shifted in January 14, 2004, when the first Hamas female suicide bomber struck. Yassin defended this change as a "significant evolution in our fight. The male fighters face many obstacles,"[38] so women can more easily reach the targets. He concluded his statement by noting that "women are like the reserve army—when there is a necessity, we use them."[39] In addition, Abd al-Asis al-Rantissi, a senior Hamas leader, stated at the end of August 2001 in an interview with Abu Tibi Television that "there is no reason that the perpetration of suicide attacks should be monopolized by men."[40] Isma'il abi Shanab, a Hamas leader in Gaza, was also eager to see women as one more weapon to inflict harm on the enemy. He stated: "Jihad against the enemy is an obligation that applies not only men, but also women. Islam has never differentiated between men and women on the battlefield."[41] The head of the Women's Activist Division of the Palestine Islamic movement Jamila Shanti argued, "Islam does not prohibit a woman from sacrificing herself to defend her land and her honour. It is she who was attacked, and she has the right to defend herself in any way. It is not puzzling that Muslim sisters have been carrying out heroic operations with Palestine since 1948. On the other hand it would be strange if the Palestinian woman had not done so, as Jihad is a personal imperative for her and no one can prevent her from waging it.[42] Some Palestinian Muslim clerics provided the religious justification for female suicide bombers.[43] Searching for new ways to resist the security complications, the Palestinians discovered that women could be an advantage and religiously backed their use.

The Palestinian Islamic Jihad (PIJ) began to launch a public campaign in 2003 to recruit women. It has focused its recruitment efforts in the northern part of the West Bank, especially in the Jenin region. Its first recruit was nineteen-year-old Heiba Daragmeh, a student at Quds Open University. Standing in from of a shopping mall in Afula on May 19, 2003, she detonated an explosive charge strapped to her body. Three civilians died in the attack and another eighty-three were injured.

Many of the Palestinian female terrorists share the experience of having lost a male relative by Israeli countermeasures. By mapping the biographies of the women who participated in the early history of the Palestinian terrorism, we could assert that some of these females were professional women with above-average

education and training, whereas others were young women with neither education nor career. Some of them were married and had children, others were single or divorced.

Two questions arise. Why did the women start to participate in the suicide bombing campaign at such a late point in time, and why are there so few females among the suicide bombers?

The answer for both questions is based partly on the generally patriarchal traditions of Muslim society, which as a whole does not promote the idea of females participating in warfare. Currently, Hamas and PIJ have enough male volunteers; and when these organizations have the chance to use a man for an attack, they prefer to do so.

It seems that Palestinian women in general have more rights and are allowed to choose political action. For instance, Rascha al-Rantissi, the widow of Hamas leader Rantissi, has run for office in Palestinian elections. Compared to other Muslim societies, Palestinian women have more opportunities and more freedom than their sisters in Iraq, Iran, Saudi Arabia, and other fundamentalist countries. They can vote, hold offices, drive cars, and own property. They also have equal access to universities. For decades, men have been fighting for the ideological goals of the terrorist organizations without having reached a substantial result. Every society has developed its identity over time and, in the Palestinian case, the concepts of a common enemy and the struggle have played a strong role in the construction of the Palestinian identity. Also, female Palestinians have learned to claim the full Palestinian identity even when that means carrying out a suicide attack. In the Muslim world, female suicide bombers have achieved immortality by becoming weapons against Israeli. When they were alive, the women who committed these actions were just women; however, from the moment they killed Israelis, they died as martyrs, achieving redemption. An important way to become a respected citizen in the Palestinian society is to kill and die.

The involvement of women in terrorism raises their awareness of the opportunities available outside the private domain. Women acquire a new understanding of their potential as political actors, and this can affect their demands within terrorist groups. Throughout the West Bank and Gaza, there are posters honoring female martyrs. Young girls no longer think of themselves as relegated to the private sphere; this in itself represents an important step toward female empowerment in Jihad.

Increased female terrorism affects women's personal and political development. Female terrorism demonstrates that traditional delineations along gender lines are unfounded and impermanent.

But this view is just one side of the coin. The phenomenon of the female suicide bomber is interconnected with a pathological misogynist culture in which young women are coerced and forced into suicide bombing in all kinds of violent and horrifying ways. Wafa Idris, for instance, couldn't bear children, and her husband divorced her. Discarded and shunned in a culture that sees a divorced barren woman as worthless, she became the obvious target of exploitation for

terrorist groups. Tahani Titit, a 24 year old Tanzim operative, explained that she desired to end her life not for nationalistic reasons but because of her father, who repeatedly beat her, and because of failed love affairs at university. Thawiya Hamour, twenty-six, from Jaba was arrested in Tulkarm on her way to perpetrate a suicide attack in Jerusalem. During her questioning, she mentioned that four months prior to her arrest she had met Mounir Halwa, who proposed marriage. Hamour's family refused this offer and, as a result, she had decided to commit a suicide terrorist attack. Titi's and Hamour's cases are classic examples of the cynical exploitation of unstable young women by terrorist organizations.

Anat Berko states, "Often wishing to clear her name, the female suicide terrorist will carry out the mission, thereby upgrading the status of her family, earning them honour and preventing their humiliation or even murder."[44] Blowing oneself up is a way to achieve respect, honor, and self-esteem in Palestinian Society. Nancy Kobrin states, "These women seek honour (sharaf) that they desire and they will never really achieve it because they are bound by female honour—*ird* which means pelvis."[45]

To conclude this section, when a Palestinian woman carries out a suicide attack or supports a terrorist organization or her male relatives, she does it for several diverse reasons. She is fighting a five-front war. These fronts are of an ideological, national, gender-based, social, and individual nature.

The incidence of female suicide bombers in Palestinian society is still in its formative stages and the foregoing analysis has shown that there is generally no single overriding motivation for a female bomber's action. Many interrelated motivations work together and create an explosive mixture that only needs some traumatic event to release all its hidden destructive energy. "A skilful terrorist operative can easily identify a candidate in this emotional state, and coolly manipulate her into becoming a weapon for his organization."[46] Palestinian women have proved to be a valuable and precious terrorism weapon as bombers and supporters.

THE WOMEN OF AL QAEDA

The roles of women in the movement of the global Salafi Jihad are similarly multifaceted. Female acts of suicide play a minor role in the Al Qaeda terrorist movement, but bin Laden's "roses" function importantly as operational facilitators, supporters of their male relatives, and ideological educators of children. Too few terrorist operations have taken place where females have been involved to derive generalizations or to identify a profile of a female Al Qaeda suicide bomber. The majority of Al Qaeda's women operate invisibly; nevertheless, they have had a strong impact on the current and next generation of terrorists. To understand their role, it is helpful to start with an analysis of Osama bin Laden's *fatawa* and other publications made by followers of the ideology. Afterward, female terrorist attacks, the concepts of sisterhood, and of the female Jihad will

be analyzed. Finally, the involvement of the women in the Al Qaeda–affiliated Jemaah Islamiah will be explained.

Until today, six *fatawa* have been identified that are allowing women to participate in martyrdom operations. The first one was issued by Yussuf al Qaradawi; three by faculty members at al-Azhar University Egypt; one by, Faysal al-Mawlawi of the European Council for Research and Legal Opinion based in Dublin; and one by Nizar Ábd al-Qadir Riyyam of the Islamic University of Gaza.[47] David Cook notes that it is significant that the more conservative Jordanian, Syrian, and Saudi religious leaders are completely absent from this list. "One can see that the question of women participating on suicide attacks has become associated with the Egyptian–Palestinian and consequently more progressive side of the Muslim world."[48]

But the ideology of the global Salafi Jihad has different functions for the women in mind than the one of a suicide bomber. The fatawa and some audiotapes of bin Laden express the role of women very clearly. In the fatwa "Declaration of War Against the Americans Occupying the Land of the Two Holy Places, Expel the Mushrikeen [infidels] from the Arabian Peninsula," he explains that women play an essential role as supporters, facilitators, and promoters in carrying out the Jihad.

> Our women had set a tremendous example for generosity in the cause of Allah; they motivate and encourage their sons, brothers and husbands to fight—for the cause of Allah in Afghanistan, Bosnia-Herzegovina, Chechnya and in other countries. . . . May Allah strengthen the belief—Imaan—of our women in the way of generosity and sacrifice for the supremacy of the word of Allah. . . . Our women instigate their brothers to fight in the cause of Allah. . . . Our women encourage Jihad saying: Prepare yourself like a struggler; the matter is bigger than the words.

However in the fatwa "Jihad Against Jews and Crusaders, World Islamic Front," published two years later, which became the manifesto of the full-fledged global Salafi Jihad, the role of women seems to be alleviated. They are mentioned once and then just addressed as being the victims of the United States and the Zionists. "Women and children, whose cry is: Our Lord, rescue us from this town, whose people are oppressors; and raise for us from thee one who will help!"

In the pledge of a training manual found by the Manchester Metropolitan Police during the search of an Al Qaeda member's home, women are also addressed as victims of the infidels: "To the sister believer whose clothes the criminals have stripped off. To the sister believer whose hair the oppressors have shaved. To the sister believer who's body has been abused by the human dogs." The ideology of the global Salafi Jihad says that a reason to carry out the defensive Jihad is when a Muslim woman is held by the *kufar* (infidels), to ensure her freedom is *fard* (duty) on the whole Muslim *ummah* (world Muslim community). But the women are also addressed as supporters "Covenant, O Sister . . . To make them desire death and hate appointments and prestige" and perpetrators

"Covenant, O Sister . . . to slaughter them like lamb and let the Nile, al-Asi, and Euphrates river flow with their blood."

In an audiotape broadcast on October 18, 2003 by Al Jazeera, bin Laden said: "Our prudent Muslim women are also expected to play their role."

A recently found document, "The role of women in the Jihad against Enemies,"[49] on a Jihadist message board written by Yussuf al-Ayyiri, who was one of the ideological leaders of the Saudi Arabian branch of Al Qaeda,[50] encourages women to take an active role in Jihad. This role does not involve active fighting, but it calls for women to encourage and support men in their active quest to join the Jihad. While explicitly stating that women should not actively engage in physical combat, the document emphasizes the power that women hold over men, reminding them that their role in Jihad is a vital necessity for the entire Muslim ummah. "The reason we address women . . . is our observation that when a woman is convinced of something, no one will spur a man to fulfill it like she will . . . The saying behind every great man stands a women was true for Muslim women at these times, for behind every great Mujahid stood a women."[51] He focuses on women as fighters, rather than in a supportive role, but he avoids making the revolutionary call of women to join in suicide operations. In the final paragraph he destroys two of the principal blocks against women actually fighting Jihad: that they would need the permission of their parents, and that women's Jihad is the performance on the *hajj* ritual.[52] As for the idea that the hajj supercedes Jihad, he cites a tradition that enumerates the importance of various activities and lists them in the following order: prayer, Jihad, and respect toward parents. "With these two comments he has laid the intellectual ground for the full participation of women in Jihad among radical Muslims."[53]

The online periodical *al-Khansaa*, which is addressed to women who share the ideology of Al Qaeda, also shows very obviously the importance of female support. This magazine says it is published by an organization called Women's Information Bureau of Al-Qaeda in the Arabian Peninsula and claims that Abdul al-Murqrin, the leader of Al Qaeda in the peninsula, and Issa Saad Mohammed bin Oushan are among the founders. Al-Khansaa bint Omar was a poetess of the pre-Islamic period who converted to Islam during the time of the Prophet Muhammad, and she is considered "the mother of the shahids." When her four sons died in the Battle of al Qadissiya, she did not mourn but thanked Allah for honoring her with their death. It was already mentioned that this archetypal picture of a mother of shahids also exists in Palestinian society. The choice of the name al-Khansaa for the magazine was not without reason. The magazine aims to motivate women to participate in Jihad by bringing up their children to be good Jihadis and by being supportive of their husbands, brothers, and sons. The magazine teaches that the goal of the woman is also to become a shahid. An editorial in the magazine states: "We love Allah and his Messenger. We march in a single path, the path of Jihad for the sake of Allah, and our goal is Shahada for the sake of Allah, and our goal is [to gain] the pleasure of Allah and His Paradise."[54]

The perception of the women is that they are standing shoulder to shoulder with their men, supporting them, helping them, and backing them up. An article titled "Obstacles in the Path of the Jihad Warrior Woman," written by Umm Badr, included indoctrination and guidelines for the women. "My noble sisters . . . The woman in the family is a mother, wife, sister and daughter. In society she is an educator, propagator and preacher of Islam, and a female jihad warrior. Mohamed Salah states that 'What is new here is the use of the medium of the Internet to recruit women.'"[55] It should be mentioned at this point that the whole ideology of the global Salafi Jihad is to build a revival of the golden age, which took place in the few years between 632 and 661. For that reason, it is not surprising that the argumentation for the role of women also derives from history. "My sister you might hear these stories and think that they have been fabricated . . . but once you will learn that even today there are women similar to those of the past, you will believe the stories about (the women in) the past."[56]

For centuries, Muslim women in different struggles and communities have joined men on the front lines of war and have died alongside with them. The most prominent example of an early Muslim in Jihad in Nusayba bint Káb, who fought in the Battle of Uhud with her husband and two sons and during the Caliphate of Abu Bakr. She joined the Muslim troops, suffered eleven wounds, and lost one arm.[57] The Prophet's own female relatives took part in Jihad. His wife Ayesha led the Battle of the Camel, and his granddaughter Zaynab bint Al fought in the Battle of Karbala. Other women were recognized for tending to the wounded, donating their jewelery for the Jihad, and encouraging their male family members to fight to ensure the survival of Islam. The involvement of the early Arab women in Jihad is celebrated today throughout the Muslim world, and they serve as icons and a precedent for the contemporary Muslim women who choose suicide operations, who have lost a family member in Jihad, or who support the ideology.

In the past, a Muslim woman was seen as the responsibility of her male relatives. Militant organizations could not recruit women directly without transgressing familial and societal honor codes that require women to seek permission for every action they take outside the family home. To secretly recruit a woman as a suicide bomber or even as a courier of messages and weapons would be seen as an insult to the family's male honor. Increasingly, this seems to be changing, as evidenced by the *al-Khansaa* article saying that women need not ask for permission to become a Jihadi because it is their duty to do so. In fact, *al-Khansaa* exploits the woman's traditional role in family and society as mother and nurturer of her children to get women to play a larger role in the Jihad.

Extremist Islamic websites are generous with advices on how women can and should participate in the Jihad. There are many suggestions on how they should bring up children to be good shahids, and what books they should read to their children to make them devout Muslims and brave fighters. These websites provide advice on how mothers, wives, and sisters of Jihadi fighters should be supportive of decisions made by their husbands to become a shahid; and how they

should provide food, shelter, and care for all shahids. That women must sacrifice their sons and husbands is a recurrent theme of much Jihadi literature.

Indeed, in some respects, females are considered to be the most effective and loyal supporters of terrorist organizations. When analyzing the women and their role in the Islamic organisation Hizb ut-Tahrir in Uzbekistan, an identical finding can be made.

Until today it has been difficult to profile female suicide bombers who have operated in name of the global Salafi Jihad, because very few cases have been observable, and there is not much known about theses women. The latest development of female suicide bombings started in Iraq in April 2003 under the command of Saddam Hussein's security forces. A car exploded in a terrorist attack at a U.S. checkpoint in western Iraq, killing three coalition soldiers. The Arabic TV station Al-Jazeera broadcast separate videotapes of the two female suicide bombers, one of them pregnant, each standing in front of the Iraqi flag, their right hands on the Korans placed on a table in front of them and their left hands brandishing automatic rifles. A woman who identified herself as "martyrdom-seeker Nour Qaddour al-Shammari" swore on the holy book of Islam "to defend Iraq . . . and take revenge from the enemies of the [Islamic] nation, Americans, imperialists, Zionists" and Arabs who have submitted to the foreigners. "We say to our leader and holy war comrade, the hero commander Saddam Hussein, that you have sisters that you and history will boast about," said the woman, who wore the red-checked *keffiyeh*, an Arab head scarf. In a separate video, another woman, who identified herself as Wadad Jamil Jassem, stood in a similar pose and declared, "I have devoted myself for Jihad for the sake of God and against the American, British and Israeli infidels and to defend the soil of our precious and dear country." The videotapes were similar to those distributed by Palestinian suicide bombers after attacks against Israelis.[58]

In September 2003, two 14-year-old girls named Imame and Sana Laghriff were arrested in Rabat, Morocco, and sentenced for terrorist offenses. According to various reports, the two were on their way to target a liquor store, with some sources suggesting this was a suicide attack plot. The twin teenagers were influenced by a branch of radical Islam advocates from a Salafia Jihadia cell.[59] It seems that the girls were highly manipulated by the male members of the cell.

Although there is little known about the other women and the intentions of their suicide attacks, the story of 19-year-old Uzbek woman, Dilnoza Holmuradova, who detonated explosives strapped to her body at Tashkent's Choru Market in March 2004, killing forty-seven people, illustrates her determination to participate in a suicide attack. Dilnoza came from a middle-class family and was an educated computer programmer and enrolled at the Tashkent police academy in 2001. She was able to speak five languages. In 2002 she began studying Islam with her elder sister, and both were greatly influenced by a meeting they had with teachers of the religion. They stopped wearing modern clothes, listening to music, and watching television. In January 2004, the sisters left their home with just two dresses and Islamic literature. Neither ever returned.[60] It is unclear when

they were recruited by the Islamic Jihad Group, a radical offshoot of the Islamic Movement of Uzbekistan.

May 2005 was the first time women were directly involved in a terrorist attack in Egypt. Two women were involved in a shooting on a tourist bus. Both were in their twenties and were related to the male perpetrator, Ihab Yassin. Negat Yassin was the suicide bomber's sister and Iman Ibrahim Khamis, his fiancée. Both women shot themselves before they could be arrested. It remains unclear if the two women intended to commit suicide or chose the tactic to evade arrest. The Abdallah-Azzam Brigades, an Al Qaeda–affiliated group, claimed responsibility for this attack.[61] The Al Qaeda–affiliated Malik Suicidal Brigades claimed responsibility for the suicide attack carried out by a women on September 28, 2005, in Talafa in northern Iraq against a U.S. military recruitment center. The group issued the statement: "A blessed sister . . . carried out a heroic attack defending her faith. . . . May God accept our sister among the martyrs."[62] In an Internet posting by Al Qaeda in Iraq, led at the time by Abu Musab Zarqawi, a Jordanian and the most feared and wanted terrorist in Iraq until he was killed by U.S. forces in 2005, said the bomber attacked the center because it was a gathering spot "of converted volunteers." Residents said the building used to be an Iraqi army recruiting center.[63] The attack seems to represent a new tactic by the terrorist groups in Iraq to use women, who are rarely searched at checkpoints because of religious and social traditions that grant women special treatment. Until recently, women have not been suspected by the security forces, and this is demonstrated by the fact that the woman who carried out the attack was dressed in men's clothing—a factor that did not lead the soldiers to pay attention to her.

On November 9, 2005, three Iraqi suicide bombers carried out attacks in Amman, Jordan, in the lobby of the Grand Hyatt Hotel, at a wedding party at the Radisson SAS Hotel down the street, and at the Days Inn. They killed fifty-six people, severely injuring ninety-three. The Jordanian security services were able to arrest Sajida Mubarark al-Rishawi. The 35-year-old Iraqi woman was the fourth suicide bomber, but her trigger cord failed and she fled the wedding reception at the Radisson. Her husband, Ali Hussein al-Shumari, also part of the suicide squad, killed himself in the bombing.[64] Her brother is Mubarak Atrous al Rishawi, at the time a senior aide to Zarqawi in western Iraq. During her confession, she gave no indication of why she wanted to carry out the attack, saying only that her husband brought her from Iraq to Jordan, showed her how to use the explosives belt and fit it onto her, telling her that it would be used to attack a hotel.[65] The Abu Musab al-Zarqawi group, the Al Qaeda in Mesopotamia, took responsibility for the blast.

In November 2006, Muriel Degauque was the first European converted Muslim woman to carry out a suicide attack. She was raised as a Roman Catholic in a suburb near Brussels in Belgium. Degauque, thirty-eight, rammed an explosives-filled vehicle into an American military patrol in the town of Baquba in Iraq on November 9, wounding one American soldier. Her story supports fears among many law enforcement officials and academics that converts to Europe's

fastest-growing religion could bring with them a disturbing new aspect in the war on terror. Women who marry Muslim men are now the largest source of religious conversions in Europe. Although a vast majority of those conversions are pro forma gestures for moderately religious in-laws, a small but growing number are women who willingly adopt the conservative comportment of their fundamentalist husbands or support them to follow the radical interpretation of Islam and join a terrorist organization belonging to the movement of Al Qaeda. French antiterrorism officials have been warning for several years that female converts represent a small but increasingly important part of the terrorist threat in Europe.

Degauque was born in the small suburb of Charleroi, a gritty coal and steel town where her father operated a crane at the sprawling smelter, according to neighbors and friends. Her parents sent her to the best local high school in the area at the time. The Belgian police say she became known as a drug user, though she was never arrested. Degauque's wayward streak took a decisive turn when her brother was killed in a motorcycle accident when she was twenty. Degauque said she should have died instead of her brother. She soon moved out of the house and began a troubled life in Charleroi. Degauque had several boyfriends after she was divorced. She eventually met an Algerian man who introduced her to Islam. She began appearing at the home of her parents wearing a head scarf. Her mother told neighbors that she was pleased because Islam had helped her daughter stop drinking and doing drugs. But her devotion became disturbing several years later after she met and married Issam Goris, the son of a Belgian man and a Moroccan woman. Goris with his long beard was already known to Belgian police as a radical Islamist. Degauque moved with him to Brussels and then to Morocco, where she learned Arabic and studied the Koran. When she returned, she wore not only a head scarf but the full-length robe. As she became increasingly rigid, she demanded that her parents follow Islamic customs when she and her husband visited.[66]

The Belgian police now say that Goris had fallen in with a group of Islamists focused on recruiting European Muslims to fight with Abu Musab al-Zarqawi's terrorist network in Iraq. The police had been monitoring the group for months when they intercepted phone calls from Goris indicating that he and his wife were already in Iraq. The police say the couple left Belgium by car and eventually entered Iraq from Syria. The Belgians didn't yet know the identities of Goris and Degauque, but they notified the United States and the Iraqi government that a Belgian couple was in the country intent on carrying out attacks. They turned over information on the telephone calls that would allow the Americans to find Goris, but Degauque struck before they found her. A day later, the Americans found Goris, who was also wrapped in explosives, apparently about to carry out an attack. They shot him before he could detonate his charges. Dismantling the network in Belgium that sent them to their deaths, police arrested another couple allegedly preparing to go to Iraq to become martyrs. The Belgian case has links to the youthful Dutch Hofstad group, a unique mix of extremist ferocity and modern European attitudes.

When analyzing these cases, it is difficult to profile female suicide bombers who operate under the banner of the global Salafi Jihad. What all these women have in common is that they were recruited and instructed by men. In three cases, the women carried out the attack shoulder to shoulder with a male relative. It could also be stated that the instance of female suicide bombers has increased over a relatively short period of time.

In addition, other findings support the observation that the involvement of women in terrorist operations is an emerging trend. In 2003, several factors led the Federal Bureau of Investigation (FBI) to prepare for the possibility that Al Qaeda might recruit women. In June 2003, the FBI started searching for a woman for the first time since the war on terror began: 31-year-old Aafia Siddiqui.[67] Along with her husband, she founded the Institute for Islamic Research and Teaching in 1999, and both were identified as suspected Al Qaeda agents. An additional indicator that the position of women is transforming is demonstrated by the warrant for a Tunisian woman, Bentiwaa Farida Ben Bechir. As a member of a cell in Italy, she was active in recruiting suicide bombers to be sent to Iraq.[68] As early as May 2003, France's famed antiterrorist investigating judge, Jean-Louis Bruguière, warned that European terrorist networks were trying to recruit Caucasian women to handle terrorist logistics, because they would be less likely to raise suspicion. On November 3, 2005, the Dutch police arrested a 21-year-old woman in Rijswijk, on suspicion of being involved in terrorist activities of the Islamist radical group Hofstad.[69] At the time of the arrest, she was on her way with her husband to kill a Dutch legislator, prominent Islam critical feminist Ayaan Hirsi Ali. The driver who brought both to the train station is also a women— a convert with cherubic Dutch looks and the former profession of police officer.[70] The women of the Dutch extremist network were new breeds of holy warriors on the front lines where Islam and the West collide. In the male-dominated world of Islamic extremism, they saw themselves as full-fledged partners in Jihad. The story of the Dutch network, fourteen members of which are on trial, reveals the increasing aggressiveness and prominence of female extremists in Europe. In a chilling trend in the Netherlands and Belgium, police are investigating the wives of militants, who are suspected of plotting suicide attacks with their husbands—or on their own. It looks like the primarily motivation of the women is to carry out a political act, and they do not follow their husbands blindly; they encourage them.

Women carry out the Jihad by educating, supporting, and encouraging their sons, brothers, and husbands. To reach this goal, they have to prepare themselves as strugglers. No less important for promoting the Salafi ideology is their role as the victims of the infidels, motivating their male relatives to carry out the Jihad. When a woman enters paradise, she will not find seventy-two male virgins waiting for her—she will sit beside her husband. A different interpretation says that the female martyr of the shahida is one of the seventy-two female virgins waiting for a male martyr. In the Shi'ite and Sunni tradition, the word *Jihad* is completely reinterpreted for the women; they might gain similar spiritual benefit for performing it, but the action performed is without topical connection to fighting.[71]

Marc Sageman discovered that 70 percent of the 400 terrorists he analyzed had been married. Every terrorist has a mother, and many of them at least one sister. Arranged marriages are a strong tradition in the Muslim world, and it would not be a mistake to assume that marriages in the global Salafi Jihad are arranged.

How intensive the women carry out the female Jihad is easy to see when analyzing the Al Qaeda affiliate Jemaah Islamiah. Sidney Jones from the International Crisis Group in Jakarta states that marriage alliances are the glue that holds Jemaah Islamiah together. "Oftentimes senior members of the organization will offer their sisters or sisters-in-law to new promising recruits so that they are not only drawn into the organization, but into the family as well." The result is that the members are much closer connected. In some cases they even had control of finances. They play a role as couriers in ensuring that, particularly after imprisonment, communication among different members of the organization is maintained. "It's not a role in actively taking part in bombing activities, the new way some of the women in Chechnya or in Sri Lanka have done. It's more ensuring that the organization stays solid."[72] The wife of the operational chief of the Jemaah Islamiah, Hambali, who was responsible for instance for the October 2002 Bali bombings, acted as his bookkeeper. The wife of Omar al-Faruk, also a key figure of the Jemaah Islamiah, translated and also acted as his bookkeeper. Both women played a crucial role in financing of the organization, as did Yazid Sufaat's wife.

Another insightful example is Malika Aroud. When her husband traveled to an Al Qaeda training camp in Afghanistan, Malika joined him. Two days before the September 11, 2001, attacks, her husband carried out a suicide bombing that killed Ahmed Shah Massoud, the leader of the north alliance in Afghanistan. Acquitted in the plot against Massoud, Malika moved to Switzerland, where she has been charged with operating a website that incited terrorism.

Women are often strongly involved in the financial issues of a terrorist organization. In the aftermath of the 9/11 attacks, the United States has closed several bank accounts of terrorist organizations or supporting institutions that were handled by women. The chance that the men will get arrested or die in combat or in an attack is much higher; so for the organization it makes sense that the individuals who take care of the financial issues have a stronger likelihood of survival. Dealing with the financial aspects could be done from home, the place where the women are usually restricted in these societies.

CONCLUSION

Over the past three years, religious terrorist groups have set the stage for the entry of female combatants. The role of women in terrorist organizations arises from the society in which they live. In patriarchal societies, women carry out attacks and support terrorist organizations as a way to have a chance to be honored by their society. But there are several motivations for women to carry out a

terrorist attack, and these reasons are interconnected. Women are motivated because they follow a violent ideology; they want to carry out a political act; look forward to regaining personal or family honor; have lost a family member;or have been manipulated in some way. There is not single rational reason that motivates female suicide bombers.

These motivations also come into play when they "just" support their male relatives in following the ideology of a terrorist organization or facilitating terrorist operations. This behavior is widespread in Muslim and Western countries. In this case, the motivation arises mainly from a process of socialization conducted in the society in which they are living, whereas in other cases they have become radicalized by themselves.

Attempts have been made to profile female suicide bombers in the hope of finding common threads in their backgrounds and motivations. It is very difficult to profile female suicide bombers or facilitators and supporters because they come from diverse educational, religious, social, and personal backgrounds.

Terrorist organizations use women as suicide bombers because they provide several considerable advantages. First, they offer a tactical advantage: stealthier attack, an element of surprise, hesitancy to search women, and the stereotype of females as being nonviolent. Second, the inclusion of women as suicide bombers increases the number of combatants. Third, this increases the publicity of an attack. Finally, women suicide bombers carry a much greater psychological impact. Suicide bombers provide a low-cost, low-technology, low-risk weapon that maximizes target destruction and instills fear. Women are even more effective with their increased accessibility and media shock value. Until today, women could rarely be found as part of the suicide bombers of the global Salafi Jihad; however, when terrorism groups find women useful in their operations, they will find or create something in the Islamic theology to justify it.

Personal and organizational motivations converge to produce an increased number of female terrorists. To the extent that these motivations persist over time, the increase in female participation in religious terrorist organizations can be expected to continue. There is a need to understand their role as operational facilitators, organizational and personal supporters, and ideological educators, as a means to develop long-term effective and efficient counterterrorism.

NOTES

1. As the meaning and usage of the word *terrorism* have changed over time to accommodate the colloquial political language and discourse of each successive era, terrorism has proved increasingly elusive in the face of attempts to find a consistent definition. Boaz Ganor provides a very fruitful definition, which will be used in this article: "Terrorism is a form of violent struggle in which violence is deliberately used against civilians in order to achieve political goals (nationalistic, socioeconomic, ideological, religious, etc.)." Boaz Ganor, *The Counter-Terrorism Puzzle: A Guide for*

Decision Makers (Somerset, NJ: Transaction, 2005), p. 17. The second phrase that needs to be explained is "global Salafi Jihad." This broad-based ideology of Al Qaeda has its roots in the Egyptian Salafi Jihad, and today it is articulated in the global Salafi Jihad. The fatwa "Jihad against Jews and Crusaders," written by Osama bin Laden and published on February 23, 1998, has become the manifesto of the full-fledged global Salafi Jihad. In this document, bin Laden extended his previous concept of jihad from a defensive to an offensive one. The global Salafi Jihad now carried the fight to the "far enemy" (the United States and the West in general), on its own territory or in third-country territory. Today, Al Qaeda is a movement of uncountable terrorist organizations, groups, and cells. The term *global Salafi Jihad* will be used to describe this movement.

2. The Free Arab Voice, exclusive interview with Leila Khaled, February 2, 1999, available at http://www.freearabvoice.org (accessed November 5, 2005).

3. Ibid.

4. Yoram Schweitzer, "Female Suicide Bombers for God," *Telavivnotes* 88 (October 9, 2003).

5. BBC News, "Woman Suicide Bomber Strikes Iraq," September 28, 2005, available http://news.bbc.co.uk/1/hi/world/middle_east/4289168.stm (accessed November 5, 2005).

6. Karla J. Cunningham, "Cross-Regional Trends in Female Terrorism," S*tudies of Conflict and Terrorism* 26 (2003), p. 172.

7. Leonard Weinberg and William Lee Eubank, "Italian Women Terrorists," *Terrorism: An International Journal* 9, no. 3 (1987), p. 242.

8. See Karla J. Cunningham, "Cross-Regional Trends in Female Terrorism," *Studies of Conflict and Terrorism* 26 (2003).

9. Barbara Victor, *Army of Roses: Inside the World of Palestinian Suicide Bombers* (New York: St. Martin's, 2003), p. 192.

10. Rhiannon Talbot, "Myths in the Representation of Women Terrorists," *Eire-Ireland* 35, no. 3–4 (Fall/Winter 2000), p. 171.

11. Sandy McEvoy, "Violent Women, Political Actors: A Feminist Analysis of Female Terror," paper presented at the International Studies Association 45th Annual Convention, March 17–20, Montreal. [AU: please cite year of presentation]

12. Clara Beyler, "Messenger of the Death: Female Suicide Bombers," International Policy Institute for Counter Terrorism, February 12, 2003, available at http://www.ict.org.il (accessed October 10, 2005).

13. Schweitzer, "Female Suicide Bombers for God."

14. Interview with Leila Khaled.

15. Weinberg and Eubank, "Italian Women Terrorists," p. 242.

16. Steven Lee Meyers, "Female Suicide Bombers Unnerve Russians," *New York Times*, (August 7, 2002), p. A1.

17. Ibid.

18. Karla J. Cunningham, "Cross-Regional Trends in Female Terrorism," *Studies of Conflict and Terrorism* 26 (2003), p. 180.

19. Vidyamali Samaranghe, "Soldiers, Housewives and Peace Makers: Ethnic Conflict and Gender in Sri Lanka," *Ethnic Studies Report* 14, no. 2 (July 1996), p. 211.

20. Ana Cutter, "Tamil Tigresses: Hindu Martyrs," Columbia University, 1998, available http://www.columbia.edu/cu/sipa/PUBS/SLANT/SPRING98/article5.html (accessed March 2, 2004).

21. Cunningham: Cross-Regional Trends in Female Terrorism," p. 181.

22. Ibid., p. 175.

23. Martha Crenshaw, "The Logic of Terrorism: Terrorist Behavior as a Product of a Strategic Choice," in *Origins of Terrorism,* ed. Walter Reich (Washington, DC: Woodrow Wilson Center Press, 1990), pp. 7–8.

24. Cunningham, "Cross-Regional Trends in Female Terrorism," p. 172.

25. Talbot, "Myths in the Representation of Women Terrorists," p. 180.

26. Ehud Talbot, "Rational Policy," *Eire-Ireland* (September–October 2000), p. 70.

27. Mia Bloom, "Feminism, Rape and War: *Engendering* Suicide Terror?" in *Dying to Kill: The Allure of Suicide Terror* (New York: Columbia University Press, 2005), p. 192.

28. Audrey Kurt Cronin, *Terrorist and Suicide Attacks*, CRS Report for Congress, Congressional Research Service, Library of Congress, August 28, 2003, Order Code RL32058, pp.14–15.

29. "It's a Woman!" *Al-Sha'ab*, February 1, 2002. cited in MEMRI Inquiry and Analysis Series, no. 84, February 13, 2002, available at http://memri.org/bin/opener.cgi?Page=archives&ID=IA8402 (accessed March 2, 2004).

30. Peter Schalk, "Women Fighters of the LTTE," *South East Asia Research* 14 (1990), p. 165.

31. Micah D. Halpern, "Terror: The Female Touch," *Israel Insider*, June 23, 2005.

32. Itamar Marcus and Barbara Crook, "The Joy of Killing Your Kids," *Palestinian Media Watch Bulletin*, March 16, 2005.

33. Ibid.

34. Nahed Habiballah, "Interviews with Mothers of Martyrs of the AQSA Intifada," *Arab Studies Quarterly* (Winter 2004).

35. Al-Khansaa was a poet in the early Islamic period. After she converted to Islam, she delivered a fiery speech encouraging her four sons to march into battle for Allah. When all four were killed, the poem she wrote was one of joy, rejoicing that Allah had honored her with deaths of her sons.

36. Armin Regular, "Mother of Two Becomes First Female Suicide Bomber for Hamas," *Haaretz* (January 16, 2004).

37. Ibid.

38. Ibid.

39. Ibid.

40. Israel Ministry of Foreign Affairs, "The Role of Palestinian Women in Suicide Terrorism," January 30, 2003, available at http://www.mfa.gov.il/MFA/MFAArchive/2000_2009/2003/1/The+Role+of+Palestinian+Women+in+Suicide+Terrorism.htm (accessed October 16, 2005).

41. Middle East News Online, January 28, 2002, available at http://www.mideasrweb.org/mewnews.htm, (accessed November 6, 2005).

42. Ibid.

43. Islamic scholars continue to debate generally whether suicide attacks against Israelis are legitimate, regardless of whether the perpetrators are men or women. The religious among those who believe them to be a legitimate form of resistance, those who organize the attacks, and those who eventually carry them out are usually associated with the radical Islamist branch of the Muslim tradition. H. Malka, "Must Innocent Die? The Islamic Debate over Suicide Attacks," *Middle East Quarterly* 10, no. 2 (Spring 2003).

44. Interview with Anat Berko, "Symposium: The She Bomber," *Front Page Magazine* (September 9, 2005).

45. Interview with Nancy Kobrin, "Symposium: The She Bomber," *Front Page Magazine* (September 9, 2005).

46. Yoni Fighel, "Palestinian Islamic Jihad and Female Suicide Bombers," October 6, 2003, available at http://www.ict.org.il (accessed January 4, 2005).

47. David Cook, "Women Fighting Jihad?" *Studies in Conflict & Terrorism* 28 (2005), p. 380.

48. Ibid.

49. Yusuf al-'Ayyiri, "Dawr al-nisa'fi jihad al-'ada," available at http://www.epri sm.org/pages/5 (accessed March 4, 2006).

50. He was killed by Saudi security forces in May 2003.

51. SITE Institute, "Document on Jihadist Message Board Calls for Women to Take Active Role in Jihad," available at http://siteinstitute.org/bin/printerfriendly/pf.cgi (accessed October 16, 2005).

52. One of the five pillars in Islam is the pilgrimage to Mecca, the hajj.

53. Cook, "Women Fighting Jihad?," p. 382.

54. Intelligence and Terrorism Information Center at the Center of Special Studies, "Al-Qa'ida Women's Magazine: Women Must Participate in Jihad," available at http://www.intelligence.org.il/eng/memri/sep_e_04.htm (accessed October 16, 2005).

55. Rawya Rageh, "Islamist Women Use the Web for War with the Infidels," *Washington Times*, August 28. 2004, available at http://washtimes.com/world/20040827-110032-4232r.htm (accessed January 4, 2005).

56. Site Institute, Document on Jihadist Message Board.

57. Assad Nimer Busool, *Muslim Women Warriors* (Chicago: Al Huda, 1995), pp. 35–37.

58. Nicole Winfield, "Women Suicide Bombers Killed Three Soldiers," *Standard Times*, available at http://www.s-t.com/daily/04-03/04-05-03/a02wn020.htm (accessed November 5, 2005); Ibrahim Khalili, "Iraqi Women Suicide Bombers," *Shia News*, available at http://www.shianews.com/hi/middle_east/news_id/0000782.php (accessed November 5, 2005).

59. BBC news, U.K. edition, "Girls Guilty of Terror Charges," September 30, 2003, available at http://news.bbc.co.uk/1/hi/world/africa/3153110.stm (accessed January 4, 2005).

60. IWPR Staff in Central Asia, "Uzbek Suicide Bombers Don't Match Terrorist Profile," April 22, 2004, ISN Security Watch, available at http://www.isn.ethz.ch/news/sw/details.cfm?ID=8709 (accessed November 5, 2005).

61. Neue Züricher Zeitung, "Verhaftungswelle nach zwei Anschlägen auf Touristen in Kairo," *Erstmals verüben Frauen ein Selbstmordattentat* no. 226, (2005), p. 1.

62. BBC News, "Woman Suicide Bomber Strikes Iraq," September 28, 2005, available at http://news.bbc.co.uk/1/hi/world/middle_east/4289168.stm (accessed November 14, 2005).

63. Jackie Spinner, "Female Suicide Bomber Attacks U.S. Military Post," *Washington Post* (September 29, 2005), available at http://www.washingtonpost.com/wp-dyn/content/article/2005/09/28/AR2005092801631.html (accessed November 5, 2005).

64. Hassan M. Fattah, "Jordan Arrests Iraqi Woman in Hotel Blasts," *New York Times* (November 14, 2005), available at http://www.nytimes.com/2005/11/14/international/middleeast/14amman.html (accessed November 14, 2005).

65. Associated Press, "U.S. Held Iraqi With Same Name as Bomber," *New York Times* (November 14, 2005), available at http://www.nytimes.com/aponline/international/AP-Iraq-Jordan.html (accessed November 14, 2005).

66. Craig S. Smith, "Raised as a Catholic, She Died as a Muslim Bomber," *New York Times* (December 6, 2005).

67. FBI, "Seeking information, Aafa Siddiqui," available at http://www.fbi.gov/terrorinfo/siddiqui.htm (accessed January 4, 2005).

68. CNN, "Italy Terror Suspect Arrested" CNN, available http://edition.cnn.com/2003/World/Europe/11/29/italy.terror (accessed January 4, 2005).

69. AFP, "Dutch Police Arrest 21-Year-Old Female Terrorist Suspect," November 3, 2005.

70. Sebastian Rotella, "Jihadi Feminism," *Jerusalem Post* (January 15, 2006).

71. Cook, "Women Fighting Jihad?," p. 377.

72. Kelly McEvers, "The Women of Jemaah Islamiah," BBC News World Edition, 2004, available at http://news.bbc.uk/2/hi/asia-pacific/3382762.stm (accessed January 4, 2005).

APPENDIX A

CIA COUNTERINTELLIGENCE: AN EXCERPT FROM THE CHURCH COMMITTEE REPORT

IX. CIA COUNTERINTELLIGENCE

A. COUNTERINTELLIGENCE: AN INTRODUCTION

1. Definition of Counterintelligence

Counterintelligence (CI) is a special form of intelligence activity, separate and distinct from other disciplines. Its purpose is to discover hostile foreign intelligence operations and destroy their effectiveness. This objective involves the protection of the United State Government against infiltration by foreign agents, as well as the control and manipulation of adversary intelligence operations. An effort is made to both discern and decive the plans and intentions of enemy intelligence services. Defined more formally, counterintelligence is an intelligence activity dedicated to undermining the effectiveness of hostile intelligence services. Its purpose is to guard the nation against espionage, other modern forms of spying, and sabotage directed against the United States, its citizens, information, and installations, at home and abroad, by infiltrating groups engaged in these practices and by gathering, storing, and analyzing information on inimical clandestine activity.[1]

Source: "Counterintelligence," in *Foreign and Military Intelligence, Final Report,* Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee), Book I, U.S. Senate, 94th Cong., 2d Sess. (April 26, 1976), pp. 163–71, written by Committee staffers John T. Elliff and Loch K. Johnson.

[1] Counterintelligence may also be thought of as the knowledge needed for the protection and preservation of the military, economic, and productive strength of the United States, including the security of the Government in domestic and foreign affairs against or from espionage, sabotage, and all other similar clandestine activities designed to weaken or destroy the United States. (Report of the Commission on Government Security Washington, D.C., 1957, pp. 48–49.)

In short, counterintelligence specialists wage nothing less than a secret war against antagonistic intelligence services. "In the absence of an effective U.S. counterintelligence program," notes a counterintelligence specialist, "[adversaries of democracy] function in what is largely a benign environment."[2]

2. The Threat

The adversaries of democracy are numerous and widespread. In the United States alone, 1,079 Soviet officials were on permanent assignment in February 1975, according to FBI figures.[3] Among these, over 40 percent have been positively identified as members of the KGB or GRU, the Soviet civilian and military intelligence units. Conservative estimates for the number of unidentified intelligence officers raise the figures to over 60 percent of the Soviet representation; some defector sources have estimated that 70 percent to 80 percent of Soviet officials have some intelligence connection.[4]

Furthermore, the number of Soviets in the United States has tripled since 1960, and is still increasing.[5] The opening of American deepwater ports to Russian ships in 1972 has given Soviet intelligence services "virtually complete geographic access to the United States," observes a counterintelligence specialist.[6] In 1974, for example, over 200 Soviet ships with a total crew complement of 13,000 officers and men called at 40 deep-water ports in this country.

Various exchange groups provide additional opportunities for Soviet intelligence gathering within the United States. Some 4,000 Soviets entered the United States as commercial or exchange visitors in 1974. During the past decade, the FBI identified over 100 intelligence officers among the approximately 400 Soviet students who attended American universities during this period as part of an East-West student exchange program.[7] Also, in the 14-year history of this program, more than 100 American students were the target of Soviet recruitment approaches in the USSR.

Other areas of counterintelligence concern include the sharp increase in the number of Soviet immigrants to the United States (less than 500 in 1972 compared to 4,000 in 1974); the rise in East-West commercial exchange visitors (from 641 in 1972 to 1,500 in 1974); and the growing number of Soviet bloc officials in this country (from 416 in 1960 to 798 in 1975).[8]

Foreign intelligence agents have attempted to recruit not only executive branch personnel, but also Congressional staff members. The FBI has advised the Committee that there have been instances in the past where hostile foreign intelligence officers have used the opportunity presented by overt contacts to attempt to recruit members of Congressional staffs who might have access to secret information.[9]

---

[2] Staff summary of interview, FBI counterintelligence specialist, 5/8/75.

[3] Staff summary of interview, FBI counterintelligence specialist, 3/10/75.

[4] FBI counterintelligence specialist (staff summary), 3/10/75.

[5] FBI counterintelligence specialist (staff summary), 5/8/75.

[6] *Ibid.*

[7] *Ibid*, 3/10/75.

[8] *Ibid.*

[9] FBI Memorandum for the Record, 10/30/75. Such recruitment approaches have been reported to the FBI by Congressional staff members. If the FBI otherwise learns of such recruitments, its policy is to report the facts to the appropriate Members of Congress.

The most serious threat is from "illegal" agents who have no easily detectable contacts with their intelligence service. The problem of "illegals" is summarized by the FBI as follows:

> The illegal is a highly trained specialist in espionage tradecraft. He may be a [foreign] national and/or a professional intelligence officer dispatched to the United States under a false identity. Some illegals [may be] trained in the scientific and technical field to permit easy access to sensitive areas of employment.
>
> The detection of . . . illegals presents a most serious problem to the FBI. Once they enter the United States with either fraudulent or true documentation, their presence is obscured among the thousands of legitimate emigres entering the United States annually. Relatively undetected, they are able to maintain contact with [the foreign control] by means of secret writing, microdots, and open signals in conventional communications which are not susceptible to discovery through conventional investigative measures.[10]

In several instances the FBI accomplished this most difficult assignment by carefully designed and limited mail opening programs which, if they had been authorized by a judicial warrant, might have been entirely proper. It is most unfortunate that the FBI did not choose to seek lawful authorization for such methods.[11]

This brief summary of the threat facing the American counterintelligence corps in this country is troubling enough, yet it does not take into account the worldwide scope of the problem. As an FBI counterintelligence expert states, hostile foreign intelligence services

> are alert for operational opportunities against the United States whether they occur within this country, abroad (in other countries) or in the home country itself. An operation might begin in the home country with recruitment of an American visitor; transfer to the United States with his return; and again, even later, might be transferred to a third country where the American agent may be met outside the normal reach of United States counterintelligence coverage. Regardless of the geographical location, the operation is still directed against the United States and can cause just as much damage from abroad as within our own borders.[12]

The espionage activities of the Soviet Union and other communist nations directed against the United States are extensive and relentless.[13]

To combat this threat, American counterintelligence officers have developed various sophisticated investigative techniques to (1) obtain information about foreign intelligence services, (2) protect our intelligence service, and (3) control the outcome of this subterranean struggle for intelligence supremacy. The task is difficult technically, and raises sensitive legal and ethical questions. As the CIA Deputy Director for Operations has testified, the

> U.S. counterintelligence program to be both effective and in line with traditional American freedoms must steer a middle course between blanket, illegal, frivolous and unsubstantiated

---

[10] FBI memorandum, "Intelligence Activities Within the United States by Foreign Governments," 3/20/75.

[11] Testimony of W. R. Wannall, Assistant Director, FBI, 10/21/75, p. 5; see Report on CIA and FBI Mail Opening.

[12] FBI Counterintelligence specialist (staff summary), 3/10/75.

[13] See Appendix III, Soviet Intelligence Collection and Operations Against the United States.

inquiries into the private lives of U.S. citizens and excessive restrictions which will render the Government's counterintelligence arms impotent to protect the nation from foreign penetration and covert manipulation.[14]

3. CI as Product: Information about "The Enemy"

Counterintelligence is both an activity and its product. The product is reliable information about all the hostile foreign intelligence services who attack the United States by stealth. To guard against hostile intelligence operations aimed at this nation, a vast amount of information is required. It is necessary to know the organizational structure of the enemy service, the key personnel, the methods of recruitment and training, and the specific operations.

This information must be gathered within the United States and in all the foreign areas to which U.S. interests extend. Within the intelligence service, this acquisitive activity is referred to as intelligence collection. The resulting product—pertinent information on the enemy intelligence service—is often called "raw" intelligence data. The efforts of intelligence services through the world to conceal such information from one another, through various security devices and elaborate deceptions, creates the counterintelligence specialist what James Angleton, former Chief of CIA Counterintelligence, calls a kind of "wilderness of mirrors."

4. CI as Activity: Security and Counterespionage

As an activity, CI consists of two matching halves: security and counterespionage. *Security* is the passive or defensive, side of counterintelligence. It consists basically of establishing static defenses against all hostile and concealed acts, regardless of who carries them out.

Counterespionage (CE) is the offensive, or aggressive, side of counterintelligence. It involves the identification of a specific adversary and a knowledge of the specific operation he is conducting. Counterespionage personnel must then attempt to counter these operations by infiltrating the hostile service (called penetration) and through various forms of manipulation. Ideally, the thrust of the hostile operation is turned back against the enemy. The security side of counterintelligence includes the screening and clearance of personnel and the development of programs to safeguard sensitive intelligence information (that is, the proper administration of security controls). The intelligence services try to defend three things: (1) their personnel, (2) their installations, and (3) their operations.

At the Central Intelligence Agency, the Office of Security is responsible for protection of personnel and installations, while actual operations are largely the preserve of the CI staff and the operating divisions. Among the defensive devices used for *information control* by intelligence agencies throughout the world are: security clearances, polygraphs, locking containers, security education, document accountability, censorship, camouflage, and codes. Devices for *physical security* include fences, lighting, general systems, alarms, badges and passes, and watchdogs. *Area control* relies on curfews, checkpoints, restricted areas, and border-frontier control.[15] Thus the security side of counterintelligence "is all that

[14] William Nelson testimony, 1/28/76, p. 5.

[15] Staff summary of interview, CIA security specialist, 8/20/75.

concerns perimeter defense, badges, knowing everything you have to know about your own people;" the counterespionage side "involves knowing all about intelligence services—foreign intelligence services—their people, their installations, their methods, and their operations. So that you have a completely different level of interest."[16] However, the Office of Security and the CI staff exchange information to assure adequate security systems.

5. The Penetration and the Double Agent

Several kinds of operations exist within the rubric of counterespionage. One, however, transcends all the others in importance: the penetration. A primary goal of counterintelligence is to contain the intelligence service of the enemy. To do so, it is eminently desirable to know his plans in advance and in detail. This admirable, but difficult, objective may be achieved through a high-level infiltration of the opposition service. As a Director of the CIA has written, "Experience has shown penetration to be the most effective response to Soviet and Bloc [intelligence] services."[17]

Moreover, a well-placed infiltrator in a hostile intelligence service may be better able than anyone else to determine whether one's own service has been penetrated. A former Director of the Defense Intelligence Agency (DIA) has observed that the three principal programs used by the United States to meet, neutralize, and defeat hostile intelligence penetrations are: (1) our own penetrations; (2) security screening and clearance of personnel; and (3) our efforts for safeguarding sensitive intelligence information.[18] The importance of the penetration is emphasized by an experienced CIA counterespionage operative, with mixed but expressive similes: "Conducting counterespionage with penetration can be like shooting fish in a barrel;" in contrast, "conducting counterespionage without the act of penetration is like fighting in the dark."[19]

Methods of infiltrating the opposition service take several forms. Usually the most effective and desirable penetration is the recruitment of an agent-in-place.[20] He is a citizen of an enemy nation and is already in the employ of its intelligence service. Ideally, he will be both highly placed and venal. The individual, say a KGB officer in Bonn, is approached and asked to work for the intelligence service of the United States. Various inducements—including ideology—may be used to recruit him against his own service. If the recruitment is successful, the operation may be especially worthwhile since the agent is presumably already trusted within his organization and his access to documents may be unquestioned. Jack E. Dunlap, who worked at and spied on the National Security Agency (NSA) in the 1960s, is a well-known example of a Soviet agent-in-place within the U.S. intelligence service. His handler was a Soviet Air Force attaché at the Soviet Embassy in Washington. Of course, a single penetration can be worth an intelligence gold mine, as were Kim Philby for the Soviet Union and Col. Oleg Penkovsky for the United States.

Another method of infiltration is the double agent. Double agents, however, are costly and time-consuming, and they are risky. Human lives are at stake. Double agents

---

[16] Raymond Rocca deposition, 11/25/75, p. 19.

[17] Memorandum from John McCone to Chairman, President's Foreign Intelligence Advisory Board, 10/8/63.

[18] The Carroll Report on the Dunlap Case, 2/12/64.

[19] CIA/CI specialist, staff summary, 11/1/75.

[20] CIA/CI specialist, staff summary, 10/17/75.

also normally involve pure drudgery, with few dramatic results, as new information is checked against existing files. On top of this comes the difficulty of assuring against a doublecross.

Moreover, passing credible documents can be a major problem. The operations must be made interesting to the opposition. To make fake papers plausible, the genuine article must be provided now and again. Classified documents must be cleared, and this process can be painstakingly slow. Also, "this means letting a lot of good stuff go to the enemy without much in return," complains a CI officer with considerable experience.[21]

To accomplish each of these tasks, hard work, careful planning, and considerable manpower are necessary. The extraordinary manpower requirements of the double agent operation restricted the abilities of the British to run cases during the Second World War—approximately 150 double agents for the entire period of the war and no more than about 25 at any one time.[22] Moreover, their mission was eased greatly by the ability of the British to read the German cipher throughout most of the conflict.

6. The Defector

Almost as good as the agent-in-place and less troublesome than the whole range of double agents is the "defector with knowledge." Here the procedure consists of interrogation and validation of bona fides, as usual, but without the worrisome, ongoing requirements for a skillful mix of false and genuine documents and other logistical support. Though an agent-in-place is preferable because of the continuing useful information he can provide, often a man does not want to risk his life by staying in-place, especially where the security is sophisticated; his preference is to defect to safety. In other words, agents-in-place are harder to come by in systems like the Soviet bloc countries; defection is more likely.[23] In contrast, agents-in-place are more easily recruited in so-called Third World areas.

Within the United States, the interrogation of intelligence service defectors who have defected in the U.S. is primarily the responsibility of the FBI, though the CIA may have a follow-up session with the individual. Sometimes the bona fides of a defector remain disputed for many years.

CIA-recruited defectors abroad are occasionally brought to the United States and resettled. The FBI is notified and, after the CIA completes its interrogation, FBI may interrogate. CIA does not bring all defectors to the United States; only those expected to make a significant contribution. CIA generally handles resettlement not only of defectors from abroad, but also (at the request of the FBI) of defectors in the United States.

7. The Deception

The penetration or double agent is closely related to another important CE technique: the deception. Simply stated, the deception is an attempt to give the enemy a false impression about something, causing him to take action contrary to his own interests. Fooling

[21] Rocca deposition, 11/25/75, pp. 33–34.

[22] Sir John Masterman, *Double Cross System of the War of 1939–45* (New Haven: Yale University Press, 1972).

[23] Bruce Solie, deposition, 11/25/75, pp. 26–27.

the Germans into the belief that D Day landings were to be in the Pas de Calais rather than in Normandy is a classic example of a successful deception operation in World War II.[24]

Deception is related to penetration because our agents operating within foreign intelligence agencies can serve as excellent channels through which misleading information can flow to the enemy. So double agents serve both as collectors of positive intelligence and channels for deception. However, there are opportunities for deception other than our own agents; in fact, "an infinite variety" exists, according to an experienced practitioner.[25] One example: the U.S. can allow penetration of its own intelligence service, and then feed false information through him.

8. Other CI Techniques

Other counterespionage operations include surreptitious surveillance of various kinds (for instance, audio, mail, physical, and "optical"—that is, photography), interrogation (sometimes incommunicado as in the case of one defector), and provocation. Decoding clandestine radio transmission and letters with messages written in secret ink between the visible lines is part and parcel of the CE trade, as is trailing suspected agents, observing "dead drops" (the exchange of material, like documents or instructions, between a spy and his handler), and photographing individuals entering opposition embassies or at other locations. At the recent funeral of CIA agent Richard Welch, two Eastern European diplomats were discovered among the press corps snapping photographs of CIA intelligence officers attending the burial ceremony.[26] Since the focus of offensive counterintelligence is disruption of the enemy service, provocation can be an important element of CE, too. It amounts, in essence, to harassment of the opposition, such as publishing the names of his agents or sending a defector into his midst who is in reality a double agent.

9. CI as Organization

Security at CIA is the responsibility of the Office of Security, a division of the Deputy Director for Administration. Counterespionage policy is guided by the Counterintelligence Staff of the Operations Directorate (Clandestine Service). Besides setting policy, the CI Staff sometimes conducts its own operations, though most CI operations emanate directly from the various geographic divisions as the CI field personnel—through the practice of the counterintelligence discipline—attempt to guard against enemy manipulation of espionage and covert action operations.

Structurally, counterintelligence services are usually composed of two additional sections which support Security and Operations. They are the Research and the Liaison sections. Good research is critical to a good counterintelligence effort, and it may take several forms. It can involve the amassing of encyclopedic intelligence on individuals, including American citizens associated—wittingly or unwitttingly—with hostile intelligence services. Specialists say that the hallmark of a sophisticated CI service is its collection of accurate records.[27] CI research personnel also produce reports on topics of interest

[24] Masterman, *Double Cross System.*
[25] CIA counterintelligence specialist (staff summary), 11/1/75.
[26] CIA counterintelligence specialist (staff summary), 1/15/76.
[27] *Ibid*, 6/27/75.

to the specialty, including guidelines for the interrogation of defectors and current analyses on such subjects as proprietary companies used by foreign intelligence services and the structure of Soviet bloc intelligence services. CI researchers also analyze defector briefs and, in the case of compromised documents, help ascertain who had access and what damage was inflicted.

Liaison with other counterintelligence services, at home and abroad, is also vital since no effective counterintelligence organization can do its job alone. The various CI units at home are particularly important, as counterintelligence—with all its intricacies and deceptions—requires coordination among agencies and sharing of records. Unlike the totally unified KGB organization, the American intelligence service is fragmented and depends upon liaison to make operations more effective. Coordination between CIA and FBI counterintelligence units is especially critical since, in theory at least, the former has foreign jurisdiction and the latter domestic, yet they must monitor the movements of foreign spies in and out of these two jurisdictions. Sometimes this coordination fails dramatically. In 1970, for example, J. Edgar Hoover of the FBI terminated formal liaison with the CIA and all the other intelligence units in the Government because of a disagreement with the CIA on a question of source disclosure (the Thomas Riha case).[28]

Liaison with foreign intelligence services overseas can undergo strain, too. As one CI specialist has said: "There are no friendly services; there are services of friendly foreign powers."[29] Each service fears the other has been infiltrated by hostile agents and is reluctant to see national secrets go outside its own vaults. Nonetheless, cooperation does take place, since all intelligence services seek information and, with precautions, will take it where they can get it if it is useful.

The CIA will work with friendly services to uncover hostile intelligence operations, including illegals, directed at the government of the friendly service. For example, a CIA-recruited defector may reveal Soviet agents in a friendly foreign government. This information is shared with the friendly government, if there is proper protection of the source. Protection of the CIA source is paramount.

FBI counterespionage activities within the United States are supervised by the Counterintelligence Branch of the FBI Intelligence Division. The Branch is made up of four Sections, three of which direct field operations conducted by the Bureau's field offices. The fourth handles liaison with other agencies and supervises the FBI's Legal Attaches assigned to serve in the embassies in several foreign countries.

The formal structure for counterespionage coordination between the FBI and the military intelligence agencies was established in 1939 and embodied most recently in a "charter" for the Interdepartmental Intelligence Conference in 1964.[30] This formal body, chaired by the FBI Director and including the heads of the military intelligence agencies, has not played a significant decisionmaking role in recent years.

As late as 1974, some FBI officials took the position that the Bureau's counterespionage activities were not under the authority of the Attorney General, since the FBI was accountable in this area directly to the United States Intelligence Board and the National

[28] Staff summary of interview, former FBI liaison person with CIA, 8/22/75.

[29] Rocca deposition, 11/25/75, p. 43.

[30] Confidential memorandum from President Roosevelt to Department Heads, 6/26/39; memorandum from Attorney General Kennedy to J. Edgar Hoover, Chairman, Interdepartmental Intelligence Conference, 3/5/64.

Security Council. A Justice Department committee chaired by Assistant Attorney General Henry Petersen sharply rejected this view and declared

> There can be no doubt that in the area of foreign counterintelligence, as in all its other functions, the FBI is subject to the power and authority of the Attorney General.[31]

In recent years the FBI has taken steps to upgrade its counterespionage effort, which had been neglected because of the higher priority given to domestic intelligence in the late 60s and early 70s.[32] New career development and mid-career training programs have been instituted. FBI agents specializing in counterespionage begin their careers as criminal investigators and not as analysts; and Bureau officials stress that their role is accurate fact-finding, rather than evaluation. Nevertheless, counterespionage supervisory personnel have recently attended high-level training courses in foreign affairs and area studies outside the Bureau.[33]

Here, then, are the key elements of counterintelligence. Together they combine into a discipline of great importance, for the rock bottom obligation of an intelligence service is to defend the country; meeting this obligation is the very *raison d'être* of counterintelligence. The discipline also represents the most secret of secret intelligence activities—the heart of the onion. Its great importance and its ultra secrecy make counterintelligence an area of concern that cannot be ignored by policymakers and by those responsible for legislative oversight. As a review of current issues in CI attests, the discipline has several problems which demand the attention of those charged with the defense of the country and the reform of the intelligence community.

---

[31] Report of the Petersen Committee on COINTELPRO, pp. 34–35. The committee was especially concerned that the *ad hoc* equivalent of the U.S. Intelligence Board had approved the discredited "Huston Plan" in 1970. However, the committee complied with the FBI's request that it exclude from its review of domestic COINTELPRO activities the Bureau's "extremely sensitive foreign intelligence collection techniques." (Memorandum from FBI Director Kelley to Acting Attorney General Robert Bork, 12/11/73.)

[32] C. D. Brennan testimony, Hearings, Vol. 2, p. 117.

[33] W. R. Wannall testimony, 1/21/76, pp. 18–22.

APPENDIX B

THE HUSTON PLAN

Editor's note: In 1970, the Nixon administration assigned a young White House aide, Tom Charles Huston, to write a report on youthful anti–Vietnam War protesters and how intelligence could be gathered about their activities. The result was a master spy plan to conduct espionage against the protesters: opening their mail, wiretapping their telephone, shadowing their every move—all without proper warrants and in violation of their first amendment rights to peaceful dissent. The major intelligence chiefs at the time approved the plan, including the DCI (Richard Helms), the FBI Director (the legendary J. Edgar Hoover), the NSA director, and the DIA director, even though the envisioned activities were in violation of the law. The plan was rescinded by President Nixon when Hoover finally decided it was too risky and complained to the President. Many of these operations went on anyway, culminating in the 1975 investigations into illegal domestic surveillance after word of the CIA's mail-opening operations leaked to the *New York Times* in 1974. The Huston Plan represents domestic counter-intelligence at the extreme, just as Iran-*contra* represents the overzealous use of covert action.

Source: *Final Report,* Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee), Book I, U.S. Senate, 94th Cong., 2d Sess. (April 26, 1976).

SPECIAL REPORT INTERAGENCY COMMITTEE ON INTELLIGENCE (AD HOC)[1]

CHAIRMAN J. EDGAR HOOVER

JUNE, 1970

[1] Under criteria determined by the Committee, in consultation with the White House, the Department of Defense, the Department of Justice, the Central Intelligence Agency, and the Federal Bureau of Investigation, certain materials have been deleted from those documents, some of which were previously classified, to maintain the internal operating procedures of the agencies involved, and to protect intelligence sources and methods. Further deletions were made with respect to protecting the privacy of certain individuals and groups. These deletions do not change the material content of these exhibits.

JUNE 25, 1970

This report, prepared for the President, is approved by all members of this committee and their signatures are affixed hereto.

Director, Federal Bureau of Investigation
Chairman

Director, Central Intelligence Agency

Director, Defense Intelligence Agency

Director, National Security Agency

PREFACE

The objectives of this report are to: (1) assess the current internal security threat; (2) evaluate current intelligence collection procedures; identify restraints under which U. S. intelligence services operate; and list the advantages and disadvantages of such restraints; and (3) evaluate current interagency coordination and recommend means to improve it.

The Committee has attempted to set forth the essence of the issues and the major policy considerations involved which fall within the scope of its mandate.

TABLE OF CONTENTS

PART ONE
SUMMARY OF INTERNAL SECURITY THREAT

I. Militant New Left Groups

A. ASSESSMENT OF CURRENT INTERNAL SECURITY THREAT

The movement of rebellious youth known as the "New Left," involving and influencing a substantial number of college students, is having a serious impact on contemporary society with a potential for serious domestic strife. The revolutionary aims of the New Left are apparent when their identification with Marxism-Leninism is examined. They pointedly advertise their objective as the overthrow of our system of government by force and violence. Under the guise of freedom of speech, they seek to confront all established authority and provoke disorder. They intend to smash the U. S. educational system, the economic structure, and, finally, the Government itself. New left groups do not have a large enough number of rank-and-file followers, nor dry they have a unity of purpose to carry out massive or paralyzing acts of insurrection. They do, on the other hand, have the will to carry on more militant efforts in local situations and an inclination to utilize more extreme means to attain their objectives.

1. *Student Protest Groups*. The Students for a Democratic Society (SDS) has, in the past year, split into several factions, including the Revolutionary Youth Movement (RYM), which has control over 30 chapters; and the Worker Student Alliance (WSA), which consists of 63 chapters. The WSA faction, dominated by the Progressive Labor Party (PLP), aims to build a worker-student movement in keeping with the PLP's aim of developing a broad worker-based revolutionary movement in the United States.

There are some 85 unaffiliated SDS chapters generally sympathetic to revolutionary tactics and goals. The trend of increased radical campus organizations is noticeable at campuses where recognition of SDS has been refused or rescinded and SDS members have banded together, with or without sanction, under a new title to attract student support. In addition, numerous ad hoc groups have been established on campuses and elsewhere to exploit specific issues.

The National Student Strike (NSS), also known as the National Strike Information Center, was formed following the entry of the United States forces into Cambodia and the deaths of four students at Kent State University. NSS, which helped to coordinate the nationwide student strike in May, 1970, has three regional centers and includes among its leadership SDS members and other New Left activists. The NSS has established a nationwide communications system of "ham" radio stations on campuses to encourage student demonstrations and disruptions. This communications capability may have a significant impact on campus stability in the coming school year.

The Venceremos Brigade (VB), established to send United States youth to Cuba to aid in the 1970 harvests, has continually received favorable publicity in Cuban propaganda media. To date, over 900 members of the VB have visited Cuba and another group of approximately 500 members are expected to follow suit. While in Cuba, VB members were individually photographed and questioned in detail about their backgrounds. Because of their contacts with Cuban officials, these individuals must be considered as potential recruits for Cuban intelligence activities and sabotage in the United States.

The greatest threat posed to the security of the country by student protest groups is their potential for fomenting violence and unrest on college campuses. Demonstrations have triggered acts of arson by extremists against war-oriented research and ROTC facilities and have virtually paralyzed many schools. There has been a growing number of noncampus, but student-related, acts of violence which increase tensions between "town and gown" and which constitute a marked escalation of the scope and level of protest activities. Few student protests are currently related to exclusively campus issues; virtually all involve political and social issues. Increasingly, the battlefield is the community with the campus serving primarily as a staging area.

The efforts of the New Left aimed at fomenting unrest and subversion among civil servants, labor unions, and mass media have met with very limited success, although the WSA and its parent, the PLP, have attempted through their "Summer Work-Ins" to infiltrate and radicalize labor. The inability of these groups to subvert and control the mass media has led to the establishment of a large network of underground publications which serve the dual purpose of an internal communication network and an external propaganda organ.

Leaders of student protest groups have traveled extensively over the years to communist countries; have openly stated their sympathy with the international communist revolutionary movements in South Vietnam and Cuba; and have directed others into activities which support these movements. These individuals must be considered to have potential for recruitment and participation in foreign-directed intelligence activity.

2. *Antiwar Activists*. The impetus and continuity for the antiwar movement is provided by the New Mobilization Committee to End the War in Vietnam (NMC) and the Student Mobilization Committee to End the War in Vietnam (SMC). The NMC is a coalition of numerous antiwar groups and individuals including communist "old left" elements. The SMC is under the control of the Trotskyist Socialist Workers Party (SWP).

The NMC and SMC have announced a policy of "nonexclusion" which places no limitation on the type of individuals allowed to participate in demonstrations. This policy opens the door for violence-prone individuals who want to capitalize on the activities of these groups. Both groups profess to follow a policy of nonviolence; however, the very nature of the protests that they sponsor sets the stage for civil disobedience and police confrontation by irresponsible dissident elements. Various individuals in NMC and SMC are calling for more militant protest activities, a subject to be discussed at national meetings by both groups in late June, 1970.

Although antiwar groups are not known to be collecting weapons, engaging in paramilitary training, or advocating terrorist tactics, the pro-Hanoi attitude of their leaders, the unstable nature of many NMC advocates and their policy of "nonexclusion" underscore the use of the antiwar movement as a conduit for civil disorder. This is further emphasized by the NMC leadership's advocacy of civil disobedience to achieve desired objectives.

There is no indication that the antiwar movement has made serious inroads or achieved any more than a slight degree of influence among labor unions, the mass media, and civil servants. One group, however, the Federal Employees for a Democratic Society (FEDS), offers a means of protest for recent radical graduates employed by the Federal Government.

The military and educational institutions are the prime targets of the anitwar movement. In addition to vandalism, arsons, and bombings of ROTC facilities, there has been

stepped-up activity to spread antiwar sympathy among American servicemen from within through sympathetic members in the military and from without through such programs as "GI Coffeehouses" and the proposed National GI Alliance. The increasing access by members of the military to the underground press, the establishment of servicemen's unions, and organizations which facilitate desertions, have contributed significantly to the increasing instances of dissent in the military services.

NMC and SMC leaders are constantly speaking before student groups and endeavoring to use student radicals to further the antiwar movement. They have called for an end to the ROTC and have demonstrated, often violently, to force universities to halt war-related research projects.

The NMC maintains close contact with the World Council for Peace and Stockholm Conference on Vietnam. A new organization dominated by NMC leaders, the Committee of Liaison with Families of Servicemen Detained in North Vietnam, emerged in January, 1970, after contacts with North Vietnamese representatives. It attempts to present a favorable picture of North Vietnamese treatment of American prisoners of war.

NMC leaders have frequently traveled abroad. It is therefore necessary to consider these individuals as having potential for engaging in foreign-directed intelligence collection.

The Central Intelligence Agency (CIA), in its analysis of bloc intelligence, is of the view that the Soviet and bloc intelligence services are committed at the political level to exploit all domestic dissidents wherever possible. This attack is being conducted through recruited agents, agents of influence, and the use of front groups. It is established bloc policy to deploy its forces against the United States as "the main enemy" and to direct all bloc intelligence forces toward ultimately political objectives which disrupt U. S. domestic and foreign policies.

3. *New Left Terrorist Groups*. The Weatherman terrorist group, which emerged from a factional split of SDS during the Summer of 1969, is a revolutionary youth movement which actively supports the revolutionary leadership role of the Negro in the United States. It has evolved into a number of small commando-type units which plan to utilize bombings, arsons, and assassinations as political weapons.

There has been evidence of Weatherman involvement in terrorist tactics, including the accidental explosion of a "Weatherman bomb factory" in New York City on March 6, 1970; the discovery of two undetonated bombs in Detroit police facilities on the same date; and the blast at New York City police installations on June 9, 1970.

While Weatherman membership is not clearly defined, it is estimated that at least 1,000 individuals adhere to Weatherman ideology. In addition, groups such as the White Panther Party, Running Dog, Mad Dog, and the Youth International Party (Yippies) are supporters of Weatherman terrorism but have no clearly definable ideology of their own.

Adherents to Weatherman ideology are also found within radical elements on campuses, among those living in off-campus communes, among New Left movement lawyers and doctors, and the underground press. Individuals who adhere to the Weatherman ideology have offered support and aid to hard-core Weatherman members, including 21 Weatherman members currently in hiding to avoid apprehension.

They identify themselves politically with North Vietnam, Cuba, and North Korea and consider pro-Soviet and pro-Chinese organizations as being aligned with imperialist

powers. In addition, some of the Weatherman leaders and adherents have traveled to communist countries or have met in Western countries with communist representatives.

Weatherman leaders and other members of terrorist groups are not known at this time to be involved in foreign-directed intelligence collection activity. The fugitive and underground status of many of these people, as well as their involvement in activities which would likely bring them to the attention of American authorities, would be a deterrent to contacts by foreign intelligence organizations.

B. ASSESSMENT OF CURRENT INTELLIGENCE COLLECTION PROCEDURES

1. *Scope and Effectiveness of Current Coverage.* Although New Left groups have been responsible for widespread damage to ROTC facilities, for the halting of some weapons-related research, and for the increasing dissent within the military services, the major threat to the internal security of the United States is that directed against the civilian sector of our society.

Coverage of student groups is handled primarily through live informants and it is generally effective at the national level or at major meetings of these groups where overall policy, aims, and objectives of the groups are determined.

The antiwar movement's activities are covered through the FBI by live informants in all organizations of interest. This is supported by information furnished by all members of the intelligence community and other Federal, state, and local agencies. Key leaders and activists are afforded concentrated and intensified investigative coverage on a continuing basis and, in situations where there are positive indications of violence, electronic surveillances have been implemented on a selective basis. Informant and electronic coverage does not meet present requirements.

Although several SDS chapters on college campuses which adhere to Weatherman ideology have been penetrated by live informants, there is no live informant coverage at present of underground Weatherman fugitives. There is electronic coverage on the residence of a Weatherman contact in New York City and on the residence of an alleged Weatherman member in San Francisco; however, no information has been developed concerning the whereabouts of the 21 Weatherman fugitives.

2. *Gaps in Current Coverage.* Established, long-term coverage is not available within student protest groups due to the fact that the student body itself changes yearly, necessitating a constant turnover in the informants targeted against these groups. His idealism and immaturity, as well as thee sensitive issues of academic freedom and the right to dissent, all serve to increase the risk that the student informant will be exposed as such.

Generally, day-to-day coverage of the planned activities of student protest groups, which are somewhat autonomous and disjointed, could be strengthened. Advance notice of foreign travel by student militants is particularly needed. Campus violence is generally attributable to small, close-knit extremist groups among radical students. Coverage of these latter groups is minimal.

The antiwar movement is comprised of a great many organizations and people which represent varied political, moral and ethnic beliefs. Current manpower commitments preclude optimum coverage of all antiwar activities on a day-to-day basis.

Existing coverage of New Left extremists, the Weatherman group in particular, is negligible. Most of the Weatherman group has gone underground and formed floating,

commando-type units composed of three to six individuals. The transitory nature of these units hinders the installation of electronic surveillances and their smallness and distrust of outsiders make penetration of these units through live informants extremely difficult.

Financially, the Weatherman group appears to be without a centralized source of funds. Wealthy parents have furnished funds to some of these individuals, including those in a fugitive status. Many members have also been involved in the thefts of credit and identification cards, as well as checks, and have utilized them for obtaining operating expenses.

3. *Possible Measures to Improve Intelligence Collection.* To establish effective coverage of student protest groups would require the expansion of live informant coverage of individual campus chapters of these organizations. This would entail extensive use of student informants to obtain maximum utilization of their services for the periods of their college attendance.

Because of the great number of individuals and groups in the antiwar movement, an increase in the manpower assigned to these investigations would facilitate more intensive coverage. In addition there are several key leaders involved in virtually all antiwar activities, including international contacts, against whom electronic surveillances and mail covers would be particularly effective.

Improvement of intelligence gathering against New Left terrorists depends on a combination of live informant coverage among key leaders and selective electronic surveillances. Because of the nature of the Weatherman groups, live informant coverage will most likely result through the defection of a key leader.

Extensive efforts have been undertaken which should produce of live informant capable of furnishing information as to the location of Weatherman fugitives and planned terrorist acts. In the event a commune is located, prompt installation of electronic coverage should produce similar results. Utilization of additional resources to expand and intensify this collection would be beneficial.

II. Black Extremist Movement

A. ASSESSMENT OF CURRENT INTERNAL SECURITY THREAT

1. *Black Panther Party*. The most active and dangerous black extremist group in the United States is the Black Panther Party (BPP). Despite its relatively small number of hard-core members—approximately 800 in 40 chapters nationwide—the BPP is in the forefront of black extremist activity today. The BPP has publicly advertised its goals of organizing revolution, insurrection, assassination and other terrorist-type activities. Moreover, a recent poll indicates that approximately 25 percent of the black population has a great respect for the BPP, including 43 percent of blacks under 21 years of age.

The Panther newspaper has a current circulation of approximately 150,000 copies weekly. Its pages are filled with messages of racial hatred and call for terrorist guerrilla activity in an attempt to overthrow the Government. The BPP has been involved in a substantial number of planned attacks against law enforcement officers, and its leadership is composed in large part of criminally inclined, violence-prone individuals.

Weapons are regularly stockpiled by the Party. During 1968 and 1969, quantities of machine guns, shotguns, rifles, hand grenades, homemade bombs, and ammunition were uncovered in Panther offices.

2. *New Left Support for BPP*. The BPP has received increasing support from radical New Left elements. During 1970, the BPP formed a working relationship with radical student dissenters by injecting the issue of Government "repression" of Panthers into the antiwar cause. Students for a Democratic Society (SDS) supported the BPP in a 1969 "united front against fascism." The probability that black extremists, including the BPP, will work closely with New Left white radicals in the future increases the threat of escalating terrorist activities. It would be safe to project that racial strife and student turmoil fomented by black extremists will definitely increase.

3. *BPP Propaganda Appearances*. Despite its small membership, the BPP has scored major successes in the propaganda arena. In 1969, BPP representatives spoke at 189 colleges throughout the Nation, while in 1967 there were only 11 such appearances. Although no direct information has been received to date indicating that the BPP has initiated any large-scale racial disorders, the year 1970 has seen an escalation of racial disorders across the Nation compared to 1969. This fact, coupled with an increasing amount of violent Panther activity, presents a great potential for racial and civil unrest for the future.

4. *Appeal to Military.* The BPP has made pointed appeals to black servicemen with racist propaganda. High priority has been placed on the recruitment of veterans with weapons and explosives training. The BPP has also called for infiltration of the Government. These activities, should they achieve even minimum success, present a grave threat.

5. *BPP Philosophy and Foreign Support.* The BPP relies heavily on foreign communist ideology to shape its goals. Quotations from Mao Tse-tung were the initial ideological bible of the BPP. Currently, the writings of North Korean Premier Kim II-sung are followed and extensive use of North Korean propaganda material is made in BPP publications and training. The Marxist-oriented philosophy of the BPP presents a favorable environment for support of the Panthers from other communist countries.

BPP leaders have traveled extensively abroad including visits to Cuba, Russia, North Korea, and Algeria. International operations of the BPP are directed by Eldridge Cleaver, a fugitive from United States courts. Cleaver has established an international staff in Algeria, from where communist propaganda is constantly relayed to the BPP headquarters in Berkeley, California. He has also established close ties with Al Fatah, an Arab guerrilla organization, whose leaders have reportedly extended invitations to BPP members to take guerrilla training during 1970. Cleaver, in a recent conversation, indicated that North Koreans are conducting similar training for BPP members. Radical white students in Western Europe and the Scandinavian countries have organized solidarity committees in support of the BPP. These committees are the sources of financial contributions to the Party and provide outlets for the BPP newspaper.

6. *Other Black Extremist Groups.* The Nation of Islam (NOI) is the largest single black extremist organization in the United States with an estimated membership of 6,000 in approximately 100 Mosques. The NOI preaches hatred of the white race and advocates separatism of the races. The NOI as a group has, to date, not instigated any civil disorders; however, the followers of this semi-religious cult are extremely dedicated individuals who could be expected to perform acts of violence if so ordered by the NOI head, Elijah Muhammed. When Muhammed, who is over 70 years of age, is replaced, a new leader could completely alter current nonviolent tactics of the organization. For example, Muhammed's son-in-law, Raymond Sharrieff, now among the top hierarchy of NOI, could rise to a leadership position. Sharrieff is vicious, domineering, and unpredictable.

There are numerous other black extremist organizations, small in numbers, located across the country. There is also a large number of unaffiliated black extremists who advocate violence and guerrilla warfare. One particular group, the Republic of New Africa (RNA), headquartered in Detroit, Michigan, calls for the establishment of a separate black nation in the South to be protected by armed forces. These groups, although small, are dedicated to the destruction of our form of government and consequently present a definite potential for instigating civil disorder or guerrilla warfare activity.

7. *Black Student Extremist Influence.* Black student extremist activities at colleges and secondary schools have increased alarmingly. Although currently there is no dominant leadership, coordination or specific direction between these individuals, they are in frequent contact with each other. Consequently, should any type of organization or cohesiveness develop, it would present a grave potential for future violent activities at United States schools. Increased informant coverage would be particularly productive in this area. Black student extremists have frequently engaged in violence and disruptive activity on campuses. Major universities which made concessions to nonnegotiable black student demands have not succeeded in calming extremist activities. During the school year 1969–70, there were 227 college disturbances having racial overtones. There were 530 such disturbances in secondary schools compared with only 320 during the previous school year.

8. *Foreign Influence in the Black Extremist Movement.* Although there is no hard evidence indicating that the black extremist movement is substantially controlled or directed by foreign elements, there is a marked potential for foreign-directed intelligence or

subversive activity among black extremist leaders and organizations. These groups are highly susceptible to exploitation by hostile foreign intelligence services.

Currently the most important foreign aspect of the black extremist movement is the availability of foreign asylum, especially with regard to black extremists subject to criminal prosecution in the United States. Some foreign countries, such as Cuba, provide a temporary safe haven for these individuals. Information has been received that passports and funds for travel have also been furnished by countries such as Cuba, North Korea, [still-classified section missing here] and Communist intelligence services do not, at present, play a major role in the black extremist movement; however, all such services have established contact with individual black militants. Thus, the penetration and manipulation of black extremist groups by these intelligence services remain distinct possibilities. Communist intelligence services are capable of using their personnel, facilities, and agent assets to work in the black extremist field. The Soviet and Cuban services have major capabilities available.

B. ASSESSMENT OF CURRENT INTELLIGENCE COLLECTION PROCEDURES

There are some definite gaps in the current overall intelligence penetration of the black extremist movement. For example, although there appears to be sufficient live informant coverage of the BPP [still-classified section missing here] additional penetration [still-classified section missing here] is needed. High echelon informant coverage could conceivably prevent violence, sabotage, or insurrection if such activity was planned by BPP leadership. Insufficient coverage of [still-classified section missing here] BPP is offset to some extent by technical coverage [still-classified section missing here]. Penetration of leadership levels has been hindered in part by current BPP policies which prevent rank-and-file members from advancing to leadership roles.

Improvement in coverage of BPP financial activities could be made, particularly with regard to sources of funds and records. Information received to date indicates that financial support for the BPP has been furnished by both foreign individuals and domestic sources. Thus, a deeper penetration and correlation of foreign and domestic information received is essential to a full determination of BPP finances. Coverage of BPP finances has been hampered by fact that BPP leaders handle financial matters personally.

In view of the increased amount of foreign travel and contacts by BPP leaders abroad, there is a clear-cut need for more complete coverage of foreign involvement in BPP activities.

1. *Other Black Extremist Organizations.* Informant coverage of the NOI is substantial, enabling its activities to be followed on a current basis. Coverage of militant black student groups and individuals is very limited because of the sensitive areas involved. An effective source of such coverage would be reliable, former members of the Armed Forces presently attending college. Live informant coverage, particularly with respect to the activities and plans of unaffiliated black militants, needs to be increased. More sources both in the United States and abroad in a position to determine the amount of foreign involvement in black extremist activities need to be developed. Maximum use of communication interceptions would materially increase the current capabilities of the intelligence community to develop highly important data regarding black extremist activities.

III. Intelligence Services of Communist Countries

A. ASSESSMENT OF CURRENT INTERNAL SECURITY THREAT

The threat posed by the communist intelligence services must be assessed in two areas: (1) direct intervention in fomenting and/or influencing domestic unrest; (2) extensive espionage activities.

Taken in complete context, these services constitute a grave threat to the internal security of the United States because of their size, capabilities, widespread spheres of influence, and targeting of the United States as "enemy number one." The largest and most skilled of these services is the Soviet Committee for State Security (KGB) which has roughly 300,000 personnel of whom some 10,000 are engaged in foreign operations.

1. *Intervention in Domestic Unrest.* There have been no substantial indications that the communist intelligence services have actively fomented domestic unrest. Their capability cannot, however, be minimized and the likelihood of their initiating direct intervention would be in direct relationship to the deterioration of the political climate and/or imminence of hostilities. The ingredients for a first-rate capability are present, including both the personnel and the ingrained philosophy and know-how for using such tactics.

Communist intelligence has shown a real capability to foment disorder in a number of trouble spots. The dissidence and violence in the United States today present adversary intelligence services with opportunities unparalleled for forty years. While fostering disorder and rebellion through communist parties and fronts is a potent weapon in the communist arsenal, their past success has been evident in clandestine recruitment efforts on campuses during times of unrest. H. A. R. (Kim) Philby, Guy Burgess, and Donald Maclean were all students at Cambridge during the depression period of the 1930's and were in the vanguard of what was then the New Left. Their recruitment and cooperation with Soviet intelligence wreaked havoc on British intelligence, and also compromised U. S. security in those sectors where they had authorized access.

[still-classified section missing here] For instance, about 900 members of the Venceremos Brigade, a group of American youths, recently completed a round trip to Cuba. This travel was financed by the Cuban Government. While in Cuba, they were exhorted to actively participate in United States revolutionary activities upon their return to the United States. [still-classified section missing here]

A sabotage manual, prepared in [still-classified section missing here] turned up in the hands of individuals responsible for recent bombings [still-classified section missing here]. While the potential for widespread, well-organized incidents of violence generated and controlled by the Cuban intelligence service is considered minimal, isolated occurrences of this nature must be considered probable. The [still-classified section missing here] services appear to have assumed the passive roles of observers and reporters.

The communist intelligence services maintain contacts and exert influence among a variety of individuals and organizations through the exploitation of ideological, cultural, and ethnic ties. Most of these liaisons are maintained with some degree of openness with individuals associated with the Communist Party, USA, various of its front groups, other pro-Soviet organizations, nationality groups, and foreign-language newspapers. These contacts are exploited as sources for and propaganda outlets of communist intelligence services. Regarded individually, these efforts cannot be considered a major threat to our

internal security; however, in total, they represent a sizable element of our population which can be influenced in varying degrees by communist intelligence service operations.

2. *Intelligence Operations.* Persistent and pervasive intelligence operations which have their inspiration and direction supplied by communist intelligence services represent a major threat to the internal security.

B. ASSESSMENT OF CURRENT INTELLIGENCE COLLECTION

1. *Scope and Effectiveness.* The scope of overall intelligence efforts is encompassed in the threefold goals of penetration, intelligence, and prosecution. Domestic implementation of these goals is delimited by agreement among United States intelligence agencies. Intelligence components of the United States military services are immediately concerned with protecting the integrity of their personnel and installations. [still-classified section missing here]

Methods used in these endeavors, employed in varying degrees by U.S. intelligence agencies dependent upon their specific tasks are: penetrations; defectors; double agent operations; physical, technical, and photographic surveillances; examination and analysis of overt publications; information supplied by friendly intelligence services; and COMINT.

2. *Gaps in Current Coverage* [still-classified section missing here]

IV. Other Revolutionary Groups

A. ASSESSMENT OF CURRENT INTERNAL SECURITY THREAT

1. *Communist Party*. The Communist Party continues as a distinct threat to the internal security because of its extremely close ties and total commitment to the Soviet Union. There are many thousands of people in the United States who adhere to a Marxist philosophy and agree with the basic objectives of the Communist Party although they do not identify themselves specifically with the organization. The Party receives most of its finances from the Soviet Union, adheres to Soviet policies explicitly, and provides a major outlet for Soviet propaganda. The Party will without question continue to implement whatever orders it receives from the Soviets in the future.

There is little likelihood that the Communist Party, USA, will instigate civil disorders or use terrorist tactics in the foreseeable future. Its strong suit is propaganda. Through its publications and propaganda it will continue its efforts to intensify civil disorders, and foment unrest in the Armed Forces, labor unions, and minority groups. The Party is on the periphery of the radical youth movement and is striving to strengthen its role in this movement and to attract new members through a recently formed youth organization, but it does not appear this group will achieve any substantial results for the Party in the future.

2. *Socialist Workers Party and Other Trotskyist Groups.* These organizations have an estimated membership of [still-classified section missing here] The major Trotskyist organization, the Socialist Workers Party, has attained an influential role in the antiwar movement through its youth affiliate, the Young Socialist Alliance, which dominates the Student Mobilization Committee to End the War in Vietnam and which has more than doubled its size on college campuses in the past year. Trotskyist groups have participated in major confrontations with authorities both on and off campuses and have consistently supported civil disorders. At this time they do not pose a major threat to instigate insurrection or to commit terrorist acts. The propaganda of these groups, while emphasizing student unrest, is also aimed at creating dissatisfaction in labor organizations and in the Armed Forces. The Trotskyist organizations maintain close relations with the Fourth International, a foreign-based worldwide Trotskyist movement.

4. *Puerto Rican Nationalist Extremist Groups.* The radical Puerto Rican independence movement has spawned approximately ten violently anti-American groups committed to Puerto Rican self-determination. Revolutionary violence is a major aim of the estimated [still-classified section missing here] members of these groups and if sufficiently strong, they would not hesitate to mount armed insurrection. Since July, 1967, some 130 bombings in Puerto Rico and in the New York City area have been attributed to these extremists. American-owned businesses have been the main targets, but there has been a recent upsurge of violence against U.S. defense facilities in Puerto Rico.

B. ASSESSMENT OF CURRENT INTELLIGENCE COVERAGE

1. *Scope and Effectiveness*. Coverage of the Communist [still-classified section missing here]

Coverage of theTrotskyist and [still-classified section missing here] groups [still-classified section missing here]

Current live informant coverage can furnish information on the general activities of these groups and it should serve to warn of policy changes in favor of insurrection or sabotage.

Informant penetration of the Puerto Rican independence groups provides information on the objectives of most of these organizations as well as the identities of their members. However, these sources have limited ability to provide advance information regarding violence committed by these groups or by individual members.

2. *Gaps in Current Coverage.* [still-classified section missing here]

Closer coverage at the policy-making levels of the Puerto Rican independence groups is needed to obtain more comprehensive information on persons involved in terrorist activities. The small memberships of many of these organizations is a major reason for the limited coverage.

3. *Possible Measures to Improve Intelligence Collection.* The selective use of electronic surveillances would materially enhance the intelligence coverage of the policy-making levels of these organizations. A particular benefit of electronic surveillance in the Puerto Rican field could be the development of information identifying persons involved in terrorist activities. Communications intelligence coverage and travel control measures could be improved to provide greater awareness of the travel and other activities of individuals of security interest. Through the establishment of additional informant coverage on college campuses, the involvement of these organizations in the radicalization of students could be assessed with increased accuracy.

PART TWO
RESTRAINTS ON INTELLIGENCE COLLECTION

The Committee noted that the President had made it clear that he desired full consideration be given to any regulations, policies, or procedures which tend to limit the effectiveness of domestic intelligence collection. The Committee further noted that the President wanted the pros and cons of such restraints clearly set forth so that the President will be able to decide whether or not a change in current policies, practices, or procedures should be made.

During meetings of the Committee, a variety of limitations and restraints were discussed. All of the agencies involved, Defense Intelligence Agency (DIA), the three military counterintelligence services, the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI), participated in these considerations.

In the light of the directives furnished to the Committee by the White House, the subject matters hereinafter set forth were reviewed for the consideration and decision of the President.

I. Specific Operational Restraints

A. INTERPRETIVE RESTRAINT ON COMMUNICATIONS INTELLIGENCE

Preliminary Discussion

Nature of Restriction

Advantages of Maintaining Restriction

Advantages of Relaxing Restriction
[still-classified section missing here]

B. ELECTRONIC SURVEILLANCES AND PENETRATIONS

Preliminary Discussion

The limited number of electronic surveillances and penetrations substantially restricts the collection of valuable intelligence information of material importance to the entire intelligence community.

Nature of Restrictions

Electronic surveillances have been used on a selective basis. Restrictions, initiated at the highest levels of the Executive Branch, arose as a result of the condemnation of these techniques by civil rights groups, Congressional concern for invasion of privacy, and the possibility of their adverse effect on criminal prosecutions.

Advantages of Maintaining Restrictions

1. Disclosure and embarrassment to the using agency and/or the United States is always possible since such techniques often require that the services or advice of outside personnel be used in the process of installation.

2. [still-classified section missing here]

3. Certain elements of the press in the United States and abroad would undoubtedly seize upon disclosure of electronic coverage in an effort to discredit the United States.

4. The monitoring of electronic surveillances requires considerable manpower and, where foreign establishments are involved, the language resources of the agencies could be severely taxed.

Advantages of Relaxing Restrictions

1. The U. S. Government has an overriding obligation to use every available scientific means to detect and neutralize forces which pose a direct threat to the Nation.

2. Every major intelligence service in the world, including those of the communist bloc, use such techniques as an essential part of their operations, and it is believed the general public would support their use by the United States for the same purpose.

3. The President historically has had the authority to act in matters of national security. In addition, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 provides a statutory basis.

4. Intelligence data from electronic coverage is not readily obtainable from other techniques or sources. Such data includes information which might assist in formulating foreign policy decisions, information leading to the identification of intelligence and/or espionage principals and could well include the first indication of intention to commit hostile action against the United States.

5. Acquisition of such material from COMINT without benefit of the assistance which electronic surveillance techniques can provide, if possible at all, would be extremely expensive. Therefore, this approach could result in considerable dollar savings compared to collection methods.

DECISION: Electronic Surveillances and Penetrations

_____ Present procedures should be changed to permit intensification of coverage of individuals and groups in the United States who pose a major threat to the internal security.

_____ Present procedures should be changed to permit intensification of coverage [still-classified section missing here].

_____ More information is needed.

NOTE: The FBI does not wish to change its present procedure of selective coverage on major internal security threats as it believes this coverage is adequate at this time. The FBI would not oppose other agencies seeking authority of the Attorney General for coverage required by them and thereafter instituting such coverage themselves.

C. MAIL COVERAGE

Preliminary Discussion

The use of mail covers can result in the collection of valuable information relating to contacts between U. S. nationals and foreign governments and intelligence services. CIA and the military investigative agencies have found this information particularly helpful in the past. Essentially, there are two types of mail coverage: routine coverage is legal, while the second—covert coverage—is not. Routine coverage involves recording information from the face of envelopes. It is available, legally, to any duly authorized Federal or state investigative agency submitting a written request to the Post Office Department and has been used frequently by the military intelligence services. Covert mail coverage, also known as "sophisticated mail coverage," or "flaps and seals," entails surreptitious

screening and may include opening and examination of domestic or foreign mail. This technique is based on high-level cooperation of top echelon postal officials.

Nature of Restrictions

Covert coverage has been discontinued while routine coverage has been reduced primarily as an outgrowth of publicity arising from disclosure of routine mail coverage during legal proceedings and publicity afforded this matter in Congressional hearings involving accusations of governmental invasion of privacy.

Advantages of Maintaining Restrictions

Routine Coverage:

1. Although this coverage is legal, charges of invasion of privacy, no matter how ill-founded, are possible.
2. This coverage depends on the cooperation of rank-and-file postal employees and is, therefore, more susceptible to compromise.

Covert Coverage:

1. Coverage directed against diplomatic establishments, if disclosed, could have adverse diplomatic repercussions.
2. This coverage, not having sanction of law, runs the risk of any illicit act magnified by the involvement of a Government agency.
3. Information secured from such coverage could not be used for prosecutive purposes.

Advantages of Relaxing Restrictions

Routine Coverage:

1. Legal mail coverage is used daily by both local and many Federal authorities in criminal investigations. The use of this technique should be available to permit coverage of individuals and groups in the United States who pose a threat to the internal security.

Covert Coverage:

1. High-level postal authorities have, in the past, provided complete cooperation and have maintained full security of this program.
2. This technique involves negligible risk of compromise. Only high echelon postal authorities know of its existence, and personnel involved are highly trained, trustworthy, and under complete control of the intelligence agency.
3. This coverage has been extremely successful in producing hard-core and authentic intelligence which is not obtainable from any other source. An example is a case involving the interception of a letter to a [still-classified section missing here] establishment in [still-classified section missing here] The writer offered to sell information to the [still-classified section missing here] and enclosed a sample of information available to him. Analysis determined that the writer could have given [still-classified section missing here] information which might have been more damaging.

DECISION: Mail Coverage

_____ Present restrictions on both types of mail coverage should be continued.
_____ Restrictions on legal coverage should be removed.

_____ Present restrictions on covert coverage should be relaxed on selected targets of priority foreign intelligence and internal security interest.

_____ More information is needed.

NOTE: The FBI is opposed to implementing any covert mail coverage because it is clearly illegal and it is likely that, if done, information would leak out of the Post Office to the press and serious damage would be done to the intelligence community. The FBI has no objection to legal mail coverage providing it is done on a carefully controlled and selective basis in both criminal and security matters.

D. SURREPTITIOUS ENTRY

Preliminary Discussion [still-classified section missing here]

Nature of Restrictions

Use of surreptitious entry, also referred to as "anonymous sources" and "black bag jobs," has been virtually eliminated. [still-classified section missing here]

Advantages of Maintaining Restrictions

1. The activity involves illegal entry and trespass.
2. Information which is obtained through this technique could not be used for prosecutive purposes.
3. The public disclosure of this technique would result in widespread publicity and embarrassment. The news media would portray the incident as a flagrant violation of civil rights

Advantages of Relaxing Restrictions

1. Operations of this type are performed by a small number of carefully trained and selected personnel under strict supervision. The technique is implemented only after full security is assured. It has been used in the past with highly successful results and without adverse effects.
2. Benefits accruing from this technique in the past have been innumerable [still-classified section missing here].
3. In the past this technique, when used against subversives, has produced valuable intelligence material.

DECISION: Surreptitious Entry

_____ Present restrictions should be continued.

_____ Present restrictions should be modified to permit procurement

_____ Present restrictions should also be modified to permit selective use of this technique against other urgent and high priority internal security targets.

_____ More information is needed.

NOTE: The FBI is opposed to surreptitious entry [still-classified section missing here]

E. DEVELOPMENT OF CAMPUS SOURCES

Preliminary Discussion

Public disclosure of CIA links with the National Student Association and the subsequent issuance of the Katzenbach Report have contributed to a climate adverse to

intelligence-type activity on college campuses and with student-related groups. It should be noted that the Katzenbach Report itself does not specifically restrain CIA from developing positive or counterintelligence sources to work on targets abroad.

Restrictions currently in force limit certain other elements of the intelligence community access to some of the most troublesome areas: campuses, college faculties, foreign and domestic youth groups, leftist journalists, and black militants. It is recognized that these are prime targets of communist intelligence services and that the opportunity for foreign communist exploitation increases in proportion to the weakness of a U.S. counterintelligence effort.

Nature of Restrictions

The need for great circumspection in making contacts with students, faculty members, and employees of institutions of learning is widely recognized. However, the requirements of the intelligence community for increased information in this area is obvious from the concern of the White House at the absence of hard information about the plans and programs of campus and student-related militant organizations. At the present time no sources are developed among secondary school students and, with respect to colleges and universities, sources are developed only among individuals who have reached legal age, with few exceptions. This policy is designed to minimize the possibility of embarrassment and adverse publicity, including charges of infringement of academic freedom.

Advantages of Maintaining Restrictions

1. Students, faculty members, and others connected with educational institutions are frequently sensitive to and hostile towards any Government activity which smacks of infringement on academic freedom. They are prone to publicize inquiries by governmental agencies and the resulting publicity can often be misleading in portraying the Government's interest.

2. Students are frequently immature and unpredictable. They cannot be relied on to maintain confidences or to act with discretion to the same extent as adult sources.

Advantages of Relaxing Restrictions

1. To a substantial degree, militant New Left and antiwar groups in the United States are comprised of students, faculty members, and others connected with educational institutions. To a corresponding degree, effective coverage of these groups and activities depends upon development of knowledgeable sources in the categories named. In this connection, the military services have capabilities which could be of value to the FBI.

2. Much of the violence and disorders which have occurred on college campuses have been of a hastily planned nature. Unless sources are available within the student bodies, it is virtually impossible to develop advance information concerning such violence.

3. The development of sources among students affiliated with New Left elements affords a unique opportunity to cultivate informant prospects who may rise to positions of leadership in the revolutionary movement or otherwise become of great long-range value.

4. The extraordinary and unprecedented wave of destruction which has swept U. S. campuses in the past several months and which in some respects represents a virtual effort to overthrow our system provides a clear justification for the development of campus informants in the interest of national security.

5. Contacts with students will make it possible to obtain information about travel abroad by U. S. students and about attendance at international conferences.

DECISION: Development of Campus Sources

_____ Present restrictions on development of campus and student-related sources should be continued.

_____ Present restrictions should be relaxed to permit expanded coverage of violence-prone campus and student-related groups.

_____ CIA coverage of American students (and others) traveling abroad or living abroad should be increased.

_____ More information is needed.

NOTE: The FBI is opposed to removing any present controls and restrictions relating to the development of campus sources. To do so would severely jeopardize its investigations and could result in leaks to the press which would be damaging and which could result in charges that investigative agencies are interfering with academic freedom.

F. USE OF MILITARY UNDERCOVER AGENTS

Preliminary Discussion

The use of undercover agents by the military services to develop domestic intelligence is currently limited to penetration of organizations whose membership includes military personnel and whose activities pose a direct threat to the military establishment. For example, although the Navy has approximately 54 Naval ROTC units and numerous classified Government contract projects on various campuses across the country, the Naval Investigative Service conducts no covert collection on college campuses. The same is true of the other military services.

Nature of Restrictions

The use of undercover agents by the military investigative services to develop domestic intelligence among civilian targets is believed beyond the statutory intent of the Congress as expressed in Title 10, U. S. Code, and in current resource authorizations. The Delimitations Agreement (1949 agreement signed by the FBI, Army, Navy and Air Force which delimits responsibility for each agency with regard to investigations of espionage, counterespionage, subversion and sabotage) reflects the current missions of the FBI and the military services. Further, there is a lack of assets to undertake this mission unless essential service-related counterintelligence missions are reduced. There is also concern for morale and disciplinary reactions within the services should the existence of such covert operations become known.

Advantages of Maintaining Restrictions

1. If the utilization of military counterintelligence in this mission is contrary to the intent of the Congress, discovery of employment may result in unfavorable legislation and further reductions in appropriations.

2. Lacking direct statutory authority, the use of the military services in this mission could result in legal action directed against the Executive Branch.

3. The use of military personnel to report on civilian activities for the benefit of civilian agencies will reduce the ability of the military services to meet service-connected intelligence responsibilities.

4. If expansion of the mission of the military services with regard to college campuses is to provide coverage of any significance, it will require corollary increases in resources.

5. Prosecutions for violations of law discovered in the course of military penetration of civilian organizations must be tried in civil courts. The providing of military witnesses will require complicated interdepartmental coordination to a much greater extent than the present and will serve, in the long run, to reduce security.

6. Disclosure that military counterintelligence agencies have been furnishing information obtained through this technique to nonmilitary investigative agencies with respect to civilian activities would certainly result in considerable adverse publicity. The Army's recent experience with former military intelligence personnel confirms this estimate. Since obligated service officers, first enlistees and draftees are drawn from a peer group in which reaction is most unfavorable, morale and disciplinary problems can be anticipated.

Advantages of Relaxing Restrictions

1. Lifting these restrictions would expand the scope of domestic intelligence collection efforts by diverting additional manpower and resources for the collection of information on college campuses and in the vicinity of military installations.

2. The use of undercover agents by the military counterintelligence agencies could be limited to localized targets where the threat is great and the likelihood of exposure minimal. Moreover, controlled use of trusted personnel leaving the service to return to college could expand the collection capabilities at an acceptable risk.

3. The military services have a certain number of personnel pursuing special academic courses on campuses and universities. Such personnel, who in many instances have already been investigated for security clearance, would represent a valuable pool of potential sources for reporting on subversive activities of campus and student-related groups.

DECISION: Use of Military Undercover Agents

_____ Present restrictions should be retained.

_____ The counterintelligence mission of the military services should be expanded to include the active collection of intelligence concerning student-related dissident activities, with provisions for a close coordination with the FBI.

_____ No change should be made in the current mission of the military counterintelligence services; however, present restrictions should be relaxed to permit the use of trusted military personnel as FBI assets in the collection of intelligence regarding student-related dissident activities.

_____ More information is needed.

NOTE: The FBI is opposed to the use of any military undercover agents to develop domestic intelligence information because this would be in violation of the Delimitations Agreement. The military services, joined by the FBI, oppose any modification of the Delimitations Agreement which would extend their jurisdiction beyond matters of interest to the Department of Defense.

II. Budget and Manpower Restrictions

The capability of member agencies, NSA, CIA, DIA, FBI, and the military counterintelligence services, to collect intelligence data is limited by available resources, particularly in terms of budget and/or qualified manpower. For some agencies fiscal limitations or recent cutbacks have been acute. Budgetary requirements for some agencies, other than the FBI, are reviewed and passed upon by officials who, in some instances, may not be fully informed concerning intelligence requirements.

The military services noted that cuts in budget requirements for counterintelligence activities have the effect of severely hampering the ability of these services to accomplish missions relating to coverage of threats to the national security. Budgetary deficiencies have occurred at a time when investigative work loads are increasing significantly.

Manpower limitations constitute a major restriction on the FBI's capabilities in the investigation of subversive activities. The problem is further complicated by the fact that, even if substantial numbers of Agents could be recruited on a crash basis, the time required to conduct background investigations and to provide essential training would mean several months' delay in personnel being available for use against the rapidly escalating subversive situation.

In the event, as a result of this report, additional collection requirements should be levied on the agencies involved, it would be necessary to provide for essential funding. For example, [still-classified section missing here]

DECISION: Budget and Manpower Restrictions

_____ Each agency should submit a detailed estimate as to projected manpower needs and other costs in the event the various investigative restraints herein are lifted.

_____ Each agency must operate within its current budgetary or manpower limitations, irrespective of action required as result of this report.

_____ More information is needed.

PART THREE
EVALUATION OF INTERAGENCY COORDINATION

I. Current Procedures to Effect Coordination

There is currently no operational body or mechanism specifically charged with the overall analysis, coordination, and continuing evaluation of practices and policies governing the acquisition and dissemination of intelligence, the pooling of resources, and the correlation of operational activities in the domestic field.

Although a substantial exchange of intelligence and research material between certain of the interested agencies already exists, much remains to be done in the following areas: (1) the preparation of coordinated intelligence estimates in a format useful for policy formulation; (2) the coordination of intelligence collection resources of the member agencies and the establishment of clear-cut priorities for the various agencies; and (3) the coordination of the operational activities of member agencies in developing the required intelligence.

II. Suggested Measures to Improve the Coordination of Domestic Intelligence Collection

It is believed that an interagency group on domestic intelligence should be established to effect coordination between the various member agencies. This group would define the specific requirements of the various agencies, provide regular evaluations of domestic intelligence, develop recommendations relative to policies governing operations in the field of domestic intelligence, and prepare periodic domestic intelligence estimates which would incorporate the results of the combined efforts of the entire intelligence community.

Membership in this group should consist of appropriate representatives named by the Directors of the Federal Bureau of Investigation, the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, and the counterintelligence agencies of the Departments of the Army, Navy, and Air Force. In addition, an appropriate representative of the White House would have membership. The committee would report periodically to the White House, and a White House staff representative would coordinate intelligence originating with this committee in the same manner as Dr. Henry Kissinger, Assistant to the President, coordinates foreign intelligence on behalf of the President. The chairman would be appointed by the President.

This interagency group would have authority to determine appropriate staff requirements and to implement these requirements, subject to the approval of the President, in order to meet the responsibilities and objectives described above.

DECISION: Permanent Interagency Group

_____ An ad hoc group consisting of the FBI, CIA, NSA, DIA, and the military counterintelligence agencies should be appointed and should serve as long as the President deems necessary, to provide evaluations of domestic intelligence, prepare periodic domestic intelligence estimates, and carry out the other objectives indicated above. The ad hoc group should be tasked to develop a permanent organization to carry out the objectives of this report.

_____ A permanent committee consisting of the FBI, CIA, NSA, DIA, and the military counterintelligence agencies should be appointed to provide evaluations of

domestic intelligence, prepare periodic domestic intelligence estimates, and carry out the other objectives indicated above.

_____ No further action required.

_____ More information is needed.

NOTE: The FBI is opposed to the creation of a permanent committee for the purpose of providing evaluations of domestic intelligence, however, the FBI would approve of preparing periodic domestic intelligence estimates.

APPENDIX C

THE SENATE SELECT COMMITTEE ON INTELLIGENCE REPORTS ON THE ALDRICH AMES COUNTERINTELLIGENCE FAILURE, 1994

CONCLUSIONS AND RECOMMENDATIONS

Over the months since his arrest, it has become clear that Aldrich Hazen Ames caused more damage to the national security of the United States than any spy in the history of the CIA. Ten Soviet sources of the CIA and the FBI were executed as a result of Ames' treachery and others were imprisoned. Ames has admitted to compromising over 100 intelligence operations of the CIA, FBI, military departments, and allied governments, and there are likely others he does not specifically recall. Literally thousands of classified documents—on subjects ranging from U.S. defense capabilities to international narcotics trafficking—were turned over by Ames to his KGB handlers. Although the formal assessment of the damage cased by Ames has yet to be completed, his betrayal stands as the most egregious in American history.

Obviously, something went terribly wrong. For a CIA officer to carry on espionage activities without detection for almost nine years indicates, on its face, a failure of the system. As the Committee began to look into this failure, we found a bureaucracy which was excessively tolerant of serious personal and professional misconduct among its employees, where security was lax and ineffective. And we found a system and a culture unwilling and unable—particularly in the early years of Ames' betrayal—to face, assess, and investigate the catastrophic blow Ames had dealt to the core of its operations.

The system which permitted Ames' prolonged betrayal must be changed. The country cannot afford such calamities in the future, and the CIA cannot afford further erosion of the public's confidence. In the wake of the Cold War, the CIA still has an important mission to

---

Source: Excerpted from "An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence," *Staff Report,* Select Committee on Intelligence, U.S. Senate, 103d Cong., 2d. Sess. (November 1, 1994), pp. 53–72.

perform—a mission that is vital to the national security of the United States. Like all government agencies, the CIA ultimately depends upon the support of the American people and the Congress to carry out its unique functions and maintain its unique capabilities. To restore that confidence, the CIA must deal effectively with the serious deficiencies highlighted by the Ames case.

In the discussion which follows, the Committee sets forth where we believe the system failed and what we believe should be done to correct it. In its action on the Intelligence Authorization Act for Fiscal Year 1995 (P.L. 103–359), the Committee undertook legislative remedies for many of these shortcomings by requiring coordination of counterintelligence matters with the FBI and by providing authorized investigative agencies with new authority to obtain access to financial information and travel records of federal employees who have access to classified information. While these legislative initiatives are an important beginning, far more is needed to correct the deficiencies evident in the Ames case than legislation alone can achieve.

In the end, regardless of what the Committee may recommend or what Congress may enact, fundamental change will come only if the Director of Central Intelligence, supervisors at all levels, and the employees of the CIA bring it about. The Committee intends to monitor the Agency's progress in this regard, but the leadership must come from within.

The Committee undertook its inquiry not for the purpose of assessing individual blame—which is the exclusive responsibility of the Executive branch—but rather to learn what had gone wrong and to evaluate the institutional lessons to be learned from the Ames case. Nevertheless, the Committee believes that the recent actions taken by the Director of Central Intelligence, R. James Woolsey, against past and current CIA officials implicated in the Ames case warrant comment.

On March 10 of this year, Director Woolsey appeared before the Committee in closed session to outline his interim responses to the Ames case. One area for reform which was cited by the Director was "management accountability." According to the Director: "[T]o my mind, this is very much at the heart of the entire matter." The Committee strongly shares this view.

Despite the CIA Inspector General's recommendation that 23 current and former CIA officials be held accountable for the Agency's failure to prevent and detect Ames espionage activities, Director Woolsey chose only to issue letters of reprimand to 11 individuals—7 retired and 4 current Agency employees. None of the individuals cited by the Inspector General was fired, demoted, suspended or even reassigned as a result of this case. In response to what was arguably the greatest managerial breakdown in the CIA's history, the disciplinary actions taken by the Director do not, in the collective experience and judgment of the Committee, constitute adequate "management accountability."

All Committee Members believe that the Director's disciplinary actions in this case are seriously inadequate and disproportionate to the magnitude of the problems identified in the Inspector General's report. It is clear, given the immense national security interests at stake, that there was "gross negligence"—both individually and institutionally—in creating and perpetuating the environment in which Ames was able to carry out his espionage activities for nine years without detection.

The Committee is concerned about the message that Director Woolsey's mild disciplinary actions will send to the overwhelming majority of CIA employees who are dedicated, conscientious, patriotic, and hard-working professionals, many of whom are exposed daily to risk and hardship. For the current employees who were faulted by the Inspector

General for their role in the Ames case to remain in their grades and positions falls far short of the level of accountability expected by the Committee. Indeed, in the wake of the Director's decision, many professionals within the Intelligence Community have contacted the Committee to register the same sentiment.

As this report documents, the failures evident in the Ames case were numerous and egregious. While it might be argued that the majority of individuals cited by the Inspector General were guilty of acts of omission rather than commission, the seriousness of these omissions cannot be overstated. The failures of the individuals cited by the Inspector General led to the loss of virtually all of CIA's intelligence assets targeted against the Soviet Union at the height of the Cold War. Ten of these agents were executed. The inability of the CIA to get to the bottom of these losses in a timely way was itself a significant management failure.

If there is not a higher standard of accountability established by DCIs, then a repeat of the Ames tragedy becomes all the more likely. Management accountability within the Intelligence Community should be no less than the highest levels found elsewhere in the Executive branch. Director Woolsey's actions do not meet this standard.

Having noted in strong terms the magnitude of CIA's failures, the Committee would be remiss not to point out what went right. A traitor, responsible for heinous acts of espionage, was identified and convicted. He has been imprisoned for life. In the end, this was accomplished by the work of a small group of CIA and FBI personnel who took part in what became a long and arduous inquiry—for some, lasting almost nine years. At least one member of this group appears to have pushed from the very beginning to get to the bottom of the 1985 compromises. It was his impetus that eventually put the investigation back on track in 1991. Over time, the scope and pace of the investigation had taken many twists and turns, some caused by the KGB and some by internal factors beyond the control of the investigators themselves. The commentary which follows is not intended to diminish in any way what was ultimately accomplished by this dedicated group of investigators and analysts.

Finally, the Committee notes that its recommendations are based upon the situation that pertained through early 1994. Director Woolsey has promulgated some new policies since then and has announced his intention to institute still others. While the Committee believes in general that stronger measures are needed, it is too early to pass judgment on the Director's recent actions.

THE FAILURE TO "FIX" PAST COUNTERINTELLIGENCE PROBLEMS

The counterintelligence function at the CIA is weak and inherently flawed. Despite repeated internal and external reports which have recognized a longstanding cultural problem with the counterintelligence function, CIA managers have, judging from the Ames case, failed to fix it.

In particular, the Committee was struck by the number of internal and external studies undertaken after 1985—which became known as the "Year of the Spy" following the exposure of spies John Walker, Ronald Pelton, Edward Lee Howard, and Jonathan Pollard—which pointed out the systemic and deeply-rooted problems in the CIA's conduct of counterintelligence.

As summarized by the recent report of the CIA Inspector General, these internal and external reports over the years focused on common themes:

That a counterintelligence career was held in low esteem at the CIA and did not attract high caliber officers. This was, in part, because officers gained promotions by agent recruitments, not by analyzing problems in recruitment operations;

That there was an ambiguous division of responsibility for counterintelligence among CIA offices;

That counterintelligence information was not being shared properly among CIA components; and

That CIA was reluctant to share counterintelligence information fully and in a timely manner with the FBI. (IG Report, pp. 16–22)

The poor state of counterintelligence at the CIA in the mid-1980s can be explained in part by the reaction to the so-called "Angleton era." James Angleton had been the head of the Counterintelligence Staff of the CIA from 1954 until 1974 (when he was involuntarily retired by DCI William Colby). He became convinced that the KGB had penetrated the CIA. Accordingly, Angleton was suspicious of virtually every Soviet agent who was recruited by the CIA and suspicious of every CIA officer responsible for such recruitment. On occasion, his suspicions led to CIA officers being fired without adequate justification.

While several of the officers who had been unjustly fired were later compensated, the counterintelligence function was effectively undermined by the negative reaction to Angleton's relentless pursuit of spies, particularly within the Soviet-East European (SE) Division of the Directorate of Operations, which had the principal responsibility for recruiting Soviet agents for the CIA.

In addition, there appears to have been an excessive focus within the Directorate on the recruitment of intelligence sources to the exclusion of counterintelligence concerns. Few officers wanted to go into counterintelligence because promotions and recognition came from successful recruitments, not from questioning, or identifying problems with, ongoing operations. Further, there was an image of a "corporate elite" constructed among these officers which led them to dismiss too readily the possibility of a spy among them.

By all accounts, these attitudes were prevalent within the Directorate of Operations at the time Ames sabotaged the Agency's Soviet operations in the summer of 1985, and they greatly contributed to management's failure to focus upon the CIA employees who had had access to the compromised cases (as explained in detail below).

The CIA made some efforts to address these shortcomings after "the Year of the Spy," In 1988, the head of the counterintelligence staff was made an "Associate Deputy Director" in the Directorate of Operations, and was double-hatted as the head of a new Counterintelligence Center (CIC). The CIA and FBI also signed a new Memorandum of Understanding (MOU) in 1988, which provided, at least on paper, for improved sharing of information in counterintelligence cases.

But these new bureaucratic "trappings" for the counterintelligence function did not overcome the fundamental problems which continued to be cited in reports issued in the 1990s. Despite the formation of a "lead office" for counterintelligence and the 1988 MOU with the FBI, the sharing of counterintelligence information between CIA components and with the FBI continued to be a serious problem, as was clearly evident in the Ames case.

In conclusion, the Committee finds that, despite repeated internal and external reports which recognized a longstanding cultural problem in the counterintelligence function, the CIA failed to implement adequate solutions. Indeed, the Committee believes the fundamental problems persist.

Recommendation No. 1: The Director of Central Intelligence should revise the CIA's strategy for carrying out the counterintelligence function. The Director should institute measures to improve the effectiveness of counterintelligence to include (a) establishing as a requirement for promotion among officers of the Directorate of Operations, service in a counterintelligence or counterintelligence-related position during their careers; (2) establishing incentives for service in a counterintelligence position; (3) instituting effective and comprehensive counterintelligence training for all officers of the Directorate of Operations and for appropriate officers assigned elsewhere in the CIA; and (4) ensuring adequate access to ongoing foreign intelligence operations by those charged with the counterintelligence function. The Committee will make this a "special interest area" for purposes of oversight until it is satisfied the weaknesses noted above have been adequately addressed.

THE FAILURE TO DEAL WITH SUITABILITY PROBLEMS

As the Ames case all too clearly demonstrates, the CIA Directorate of Operations is too willing to dismiss, deny, or ignore suitability problems demonstrated by its officers.

From the outset of his career at the CIA, Ames demonstrated serious suitability problems which, over the years, should have led his supervisors to reassess his continued employment. These problems included drunkenness, disregard for security regulations, and sloppiness towards administrative requirements. In the years immediately before he began to commit espionage and during the rest of his career, his supervisors were aware of his personal and professional deficiencies, but did not make his problems part of his official record, nor act effectively to correct them. Despite his recognized unsuitability, there is little evidence that his assignments, activities, or access to sensitive information were in any way limited as a result.

Prior to Ames's assignment to the counterintelligence staff of the SE Division in 1983, his supervisor in Mexico City sent a message to CIA headquarters recommending that Ames be counseled for alcohol abuse when he returned. While Ames's supervisor recognized a chronic problem, the message to headquarters apparently stemmed from an incident which occurred at an official reception at the U.S. Embassy where Ames was drunk and became involved in a loud argument with a Cuban official. On another occasion, Ames was involved in a traffic accident in Mexico City and was so drunk he could not answer police question nor recognize the U.S. Embassy officer sent to help him. In fact, based upon recent interviews with his colleagues, Ames was notorious for long, alcoholic lunches, often slurring his speech when he returned to the office. None of this behavior prompted any serious effort to correct the problem while Ames was overseas, or when he later returned to CIA headquarters.

In April 1983, when CIA headquarters asked Ames's supervisors in Mexico City whether Ames qualified for a staff position in another Latin American country, they recommended against it, citing his alcohol problem, his failure to do financial accountings, and his generally poor performance. Nevertheless, six months later, when a former supervisor of Ames requested him to fill a position in the SE Division at headquarters—the most sensitive element of the Directorate of Operations—there is no indication that Ames' alcohol problem or poor performance were ever noted. Indeed, Ames was placed in a position which provided him access to the identities of virtually all of the Soviet intelligence officers by the CIA without his new supervisors being aware of the problems he had had in Mexico City.

The alcohol abuse counseling that Ames ultimately did receive upon his return to headquarters amounted to one conversation with a counselor, who, according to Ames, told him that his case was not a serious one when compared to many others in the Directorate of Operations.

In 1983, during the assignment in Mexico City, Ames also began an extra-marital relationship with a Colombian national, Rosario Casas Dupuy (hereinafter "Rosario"), herself a recruited asset of the CIA. Over time, the seriousness of their relationship became apparent to several of Ames's colleagues, but this never led to any action by Ames's supervisors, despite the fact that CIA regulations prohibit sexual relationships with recruited assets and require that reports of "close and continuing" relationships with foreign nationals be submitted by employees. Despite the security implications of this relationship, the violation of Agency regulations was ignored.

In fact, Ames did not file an official report concerning his relationship with Rosario until April 1984, four months after she came to the United States to live with him. Indeed, it appears that until their marriage in August 1985, Ames (still married to his first wife) and Rosario continued to live together, without any perceptible concern being registered by the CIA. While the counterintelligence staff recommended in February 1985, that in view of the anticipated marriage, Ames, be moved to a less sensitive position, nothing changed. Ames continued in the same position.

While his alcohol problem abated during this assignment to the SE Division—at least as a matter of attracting official attention—it resurfaced during his assignment in Rome. He was known among colleagues for his long, alcoholic lunches, for sleeping at his desk, for often slurred speech, and generally as a marginal performer. On one occasion, after an Embassy reception, he was so drunk that he passed out on a street and awakened in a hospital. While his supervisor was unhappy, this incident did not become part of Ames' record, nor does it appear that this episode led to counseling or any serious reevaluation of Ames' fitness for continued service. Indeed, the same supervisor extended Ames' tour in Rome for a third year.

Over his career, Ames repeatedly demonstrated carelessness and disdain for security requirements. In 1975, while on his way to meet a CIA source in New York, Ames left a briefcase of classified materials identifying the source on a subway train. Although the briefcase was ultimately recovered, it might well have compromised the source's relationship with the CIA. In the fall of 1984, he brought Rosario to CIA housing where CIA undercover officers were staying, in violation of security regulations. In August 1985, he took her to the safe house where the Soviet defector Yurchenko was being debriefed, again in violation of security procedures. In Rome, he was known to prepare classified reports at home. During his assignments at CIA headquarters between 1989 and 1994, he was occasionally found in other CIA offices where he had no reason to be, and with materials he had no reason to have.

He was equally negligent throughout his career in complying with the administrative requirements imposed on officers of the Directorate of Operations, such as submitting financial accountings for the cases he was handling.

Despite these and other incidents, Ames never received a single official reprimand during his 31-year career at the CIA. Indeed, most of the incidents and shortcomings which have come to light since Ames was arrested were never made a matter of official record. Once on board, his fitness to serve in the Directorate of Operations was never reevaluated.

The Committee appreciates that intelligence officers of the Directorate of Operations are often placed in jobs and situations with stresses and strains that far exceed those of the average government employee. But these positions also demand self-control and personal discipline. Particularly in overseas assignments, it may be impossible to separate an intelligence officer's private life from his or her public, official one. A single misstep can prove his undoing or that of other officers.

It is the Committee's perception, which the Ames case confirms, that the Directorate of Operations has been far too willing to dismiss or ignore flagrant examples of personal misconduct among its officers. Excessive drinking and extra-marital relationships with sources have all too often been seen as part of the job, rather than as indicators of problems. Security concerns are too often dismissed as the bureaucratic whining of small-minded administrators. All too often an officer who has been through training, gone through the polygraph examination, and had an overseas assignment, is accepted as a "member of the club," whose fitness for assignments, promotions, and continued service becomes immune from challenge.

Director Woolsey, in a recent speech, said that the "culture" of the directorate must be changed. The Committee shares that view. Such change will not come solely by changing regulations or personnel. It will come only when supervisors at every level of the directorate take seriously their responsibilities as managers. Personal misconduct should be documented. Officers who do not meet acceptable standards of personal behavior should not be assigned to personal behavior should not be assigned to sensitive positions nor qualify for supervisory positions. Personal shortcomings should be factored into consideration of promotions and bonus awards. While officers with personal problems should be given an opportunity, as well as appropriate assistance, to rehabilitate themselves, failing that, their employment with the directorate, if not with the Agency itself, should be terminated.

Recommendation No. 2: The Director of Central Intelligence should ensure that where evidence of suitability problems comes to the attention of supervisors, it is made a matter of official record and factored into the consideration of assignments, promotions, and bonus awards; that efforts are made to counsel and provide assistance to the employee where indicated, and, if the problem persists over time, the employment of the individual is terminated. The Committee will make this a "special interest area" for purposes of oversight until it is satisfied these policies have been instituted and are being observed within the Directorate of Operations.

Recommendation No. 3: The Director of Central Intelligence should, in particular, take prompt and effective action to deal with what appears to be a widespread problem of alcohol abuse by ensuring that CIA employees experiencing such problems are identified and are put into effective counseling and/or treatment. During this period, these employees should be suspended from their duties until they have demonstrated to a qualified professional their fitness to return to service. Should their problems continue, their employment should be terminated.

Recommendation No. 4: The Director of Central Intelligence should institute, consistent with existing legal authority, an "up or out" policy for employees of the CIA, similar to that of the Foreign Service, without waiting for the report required by section 305 of the Intelligence Authorization Act for Fiscal Year 1995, pertaining to the Intelligence Community as a whole. Chronically poor performance should be grounds for dismissal from the Agency. If the Director decides not to institute such a policy and does not provide a

persuasive rationale to the Committee for his decision, the Congress should enact legislation requiring such a policy during the next Congress.

Recommendation No. 5: The Director of Central Intelligence should review and revise the performance appraisal reporting system of the CIA, to include a review of the factors upon which employees are rated and the grading system which now exists, to institute a system which reflects more accurately job performance. Where supervisors are concerned, their rating should include an assessment of how well they have supervised the performance and development of their subordinates.

THE FAILURE TO COORDINATE EMPLOYEES' OPERATIONAL ACTIVITIES

The Ames case providers a striking example of CIA supervisors failing to critically evaluate the contacts of an operations officer—with known personal shortcomings and in an extremely sensitive position—with Soviet officials in 1984 and 1985. Further, the fact that Ames virtually ceased submitting reports of such contacts, in violation of standard Agency procedures, never became known to his SE Division supervisors or made part of his official record.

In 1984, while occupying a position within the SE Division which gave him access to the identities of Soviet agents working with the CIA and FBI, Ames, with the approval of his immediate supervisor, began making contacts with Soviet Embassy officials in Washington, D.C. According to testimony received by the Committee, it was not infrequent that Directorate of Operations Officers at CIA headquarters were asked to "help out" other CIA elements that had responsibility for establishing relationships and maintaining contacts with foreign individuals located in the Washington area.

The Committee has been advised that Ames's senior supervisors in the SE Division were unaware that he was having these meetings and would have disallowed them had they known.

In any event, to permit a person in Ames's position, and someone with the personal and professional shortcomings already noted, to meet alone with Soviet Embassy officials substantially increased the risk of the disaster that eventually occurred. It provided Ames with an opportunity that he otherwise may not have had, or may have had difficulty in contriving on his own.

After June 1985, after his espionage activities had begun, Ames repeatedly failed to submit reports of his contacts with Soviet officials. While his failure prompted complaints from the FBI, the CIA element that Ames was supporting failed to bring this to the attention of his supervisors in the SE Division, nor was it reflected in his official record. Again, had Ames' SE Division supervisors been aware of his failure to file these reports, it may have alerted them to a possible problem. Since the advancement of Directorate of Operations officers depends upon their official reporting, the failure to file such reports should have suggested something was amiss.

A similar failure occurred during his assignment in Rome. While his supervisor was aware that he was meeting along with Soviet officials in Rome (one of whom was Ames' KGB contact), Ames explained his failure to file reports of such meetings on the basis that he had obtained little worthwhile information. This apparently was enough to satisfy the supervisor.

Recommendation No. 6: The Director of Central Intelligence should revise the policies and procedures governing the operational activities of CIA officers to ensure that these activities are better supervised, controlled, coordinated, and documented.

THE FAILURE TO APPLY A STRUCTURED METHODOLOGY TO THE INVESTIGATION OF INTELLIGENCE COMPROMISES

The most puzzling deficiency in the Ames case was the failure, in the wake of the 1985–86 compromises, to aggressively investigate the possibility that CIA had been penetrated by a KGB spy.

Certainly by the fall of 1986, the CIA was aware that it had suffered a disaster of unprecedented proportions which was not explained by the defection of Edward Lee Howard. Within a matter of months, virtually its entire stable of Soviet agents had been imprisoned or executed. In the days of the Cold War, Soviet operations represented the Agency's principal *raison d'etre.* There were no operations which had greater importance to its mission. The CIA was left virtually to start from scratch, uncertain whether new operations would meet the same fate as its old ones.

To be sure, these compromises involved extremely sensitive agents. There was a need for discretion in terms of how the matter was handled. But this does not explain or excuse the Agency's tentative, tepid response. Initially, some CIA officers could not believe that the KGB would "roll up" all of CIA's sources at once if the KGB had a source in the CIA who was still in place. Taking some comfort that new operations appeared to be surviving, some believed the problem had gone away. But this in no way explains the seeming lack of urgency to get to the bottom of what had gone so drastically wrong.

The obvious place to begin would have been with the CIA employees who had had access to the information which had been compromised. At least one official in the SE Division made a strong plea to his supervisors at the time that they needed to "investigate it, not study it." But this did not happen. The CIA task force created in October 1986, undertook what was largely an analytical review of the compromised cases. The task force did oversee an Office of Security review of personnel who had served in Moscow, but no broader examination was made of all CIA officers who had had access to the compromised cases. No systematic effort was made to identify and investigate problem employees and their activities, as was eventually done in 1991–92.

Later, the CIA came to suspect that the KGB was running ploys against them, purposely suggesting reasons for the compromises other than a penetration of the CIA itself. Even then, however, any sense of urgency was lacking. CIA analysts waited for things to happen, for more information to surface. They continued to analyze and conjecture. There was no clear sense of purpose, no clear methodology, and no clear sense of what was required to get to the bottom of the compromises.

In a related counterintelligence investigation of a report suggesting that the KGB may have recruited a source in a particular office in the CIA, a CIA investigator conducted a systematic investigation of over 90 employees who were assigned to that office. The inquiry took more than year. But investigators did not conduct the same type of inquiry of the CIA employees who had had access to the information that was actually compromised in 1985 until 1991–1992.

The FBI was officially brought into the case in October 1986, when the CIA learned that two sources recruited by the FBI had been compromised. But the two agencies worked

their investigations separately, despite the likelihood that the compromises were caused by the same source (whether it be human or technical).

While the FBI and CIA task forces regularly exchanged information on the compromises and on the progress of their respective analyses, they never performed a systematic assessment, together, of the CIA employees who had had access to the compromised information, until mid-1991.

Why CIA management during the 1986–1991 period did not attach more importance or urgency to getting to the bottom of the 1985 compromises is incomprehensible to the Committee. While CIA Director William Casey and Deputy Director for Operations (DDO) Clair George, who were in office at the time the compromises occurred, reportedly regarded them as "a huge problem," the Agency's response was to create a 4-person team to analyze the problem. No one believed there was a basis for bringing in investigators from the FBI at this juncture, apparently because CIA was unable to pin responsibility on a particular CIA employee.

While Casey and George became deeply enmeshed in the Iran-contra scandal in the fall of 1986 and spring of 1987, this circumstance does not explain, in the view of the Committee, why a problem so close to the heart of the CIA's mission was not given more attention by senior management. Indeed, once Casey and George departed the scene, it does not appear that their successors—either as DCI or as DDO—gave the inquiry any particular emphasis or priority. DCI William Webster, his deputy Robert M. Gates, and the new DDO Richard Stolz were briefed on the compromises in 1988, but did not delve deeply into either the nature of the problem (which was now several years old) or what the Agency was doing to resolve it.

Due to the extraordinary sensitivity of this inquiry, there was only one junior investigator from the Office of Security assigned to the case from 1985 until 1991. He was responsible for investigating all counterintelligence leads and reports coming in which involved CIA employees. After he began to develop information regarding Ames' unexplained affluence in the fall of 1989, he was diverted from this investigation for a nine-month period, first for training and then to handle other leads. There was no one else assigned to pick up the Ames leads. Nor was consideration given to having the FBI pick up the leads, despite the fact that the information now focused upon a particular CIA employee within the United States.

While the Committee believes that the investigator in question made a good faith effort to work the leads he was given, he was essentially self-trained and, because of the compartmented nature of the investigation, was given very little help and guidance. Overworked and overloaded, he did not use all of the investigative techniques he might have utilized to get at Ames' financial situation. Indeed, the statutory authority invoked by the CIA in 1992 to obtain access to Ames' bank records was available to the Agency in 1989. Had this authority been utilized at the time information was received concerning Ames's unexplained affluence, in might well have led to his detection at a much earlier stage. The investigator also apparently made no effort to develop information regarding Ames's unexplained affluence during his assignment in Rome. Efforts to verify the financial condition of Ames's in-laws in Bogota were shoddy and ineffective, producing inaccurate information which supported rather than exposed Ames's contrived explanation.

The Committee does not think it fair to hold the investigator assigned to the case solely responsible for these failures. CIA managers simply failed to assign enough investigators

to such an important task and failed to provide them with sufficient legal and administrative support to ensure that all appropriate avenues would be explored and all appropriate investigative authorities utilized. Since the professional investigative expertise of the FBI was effectively spurned during this period, insufficient resources and expertise were brought to bear on the case.

The Committee believes that those in charge of the CIA during the 1986–1991 period—Director William Casey, Acting Director and later Deputy Director Robert Gates, Director William Webster, and Deputy Director and later Acting Director Richard Kerr—must ultimately bear the responsibility for the lack of an adequate investigative response to the 1985 compromises. Whatever they may have personally understood the situation to be, they were in charge. It was their responsibility to find out what was being done to resolve the 1985 compromises. Based upon the information available to the Committee, they failed to do so.

Their failure is especially disheartening when one realizes that the information developed in August 1992, which finally focused the investigation on Ames—correlating his bank deposits in 1985 and 1986 with his meetings with Soviet officials—was available to investigators since 1986. Unfortunately, no one asked for it, even when alerted to Ames's unexplained affluence in October 1989.

Although the 1985–86 compromises represented a unique situation for the CIA, the Ames case demonstrates the lack of a clear *modus operandi* for dealing with situations where intelligence sources are known to have been compromised.

Recommendation No. 7: The Director of Central Intelligence should establish procedures for dealing with intelligence compromises. At a minimum, these procedures should entail a systematic analysis of all employees with access to the relevant information and, if suspects are identified, provide an investigative methodology to determine whether there is evidence of unexplained affluence, unreported travel, unreported contacts, or other indicators of possible espionage. This type of systematic analysis should begin when a known compromise occurs, not after CIA has eliminated the possibility of a technical penetration, or after CIA has narrowed the range of possible suspects to one or two employees. Analysis and investigation should be undertaken on the basis of access and opportunity, and should not be delayed waiting for evidence on culpability.

Recommendation No. 8: Pursuant to section 811 of the Intelligence Authorization Act for Fiscal Year 1995, the FBI should be notified immediately of any case where it is learned that an intelligence source has been compromised to a foreign government, regardless of whether the CIA believes at the time that there is a basis for an FBI counterintelligence or criminal investigation of a particular employee or employees. The CIA should also coordinate with the FBI subsequent investigative actions involving employees potentially involved in the case in order not to prejudice later criminal or counterintelligence activities of the FBI and in order to benefit from the investigative assistance and expertise of the FBI.

Recommendation No. 9: The Director of Central Intelligence should require that all employees assigned as counterintelligence investigators have appropriate training, experience, and supervision which ensures, at a minimum, such investigators will be familiar with, and know how to utilize, the investigative authorities available to the CIA and the FBI.

Recommendation No. 10: CIA management must ensure that adequate analytical and investigative resources are assigned to counterintelligence cases, and that other kinds of staff assistance (e.g., legal support, administrative support) are made available. In turn,

those involved in these cases must ensure that their needs are communicated to their supervisors. The Inspector General of the CIA should periodically assess the counterintelligence cases of the CIA to ensure that adequate resources are being afforded to particular cases.

Recommendation No. 11: The status of significant counterintelligence investigations must be regularly briefed to senior Agency officials, including the Director of Central Intelligence. Such briefings should include an explanation of the resources and expertise being brought to bear upon a particular case.

THE FAILURE TO EXPEDITE THE INQUIRY AFTER 1991

The period after the CIA and FBI decided to join forces in June 1991—compared with the period between 1985 and 1991—was relatively intense and focused. For the first time, investigators conducted a systematic review of the CIA employees who had had access to the compromised information, and there was an intensive, productive effort to link Ames and other priority suspects to the compromises.

Yet even during this phase, the investigation took an inordinate amount of time and was plagued by past inefficiencies. The joint investigative unit still had only four people (two from each agency); and there was still a lone CIA investigator working with them. While members of the joint investigative unit did obtain support from the CIA Office of Security and the FBI Washington Metropolitan Field Office, they were still but a few people carrying an extraordinarily demanding workload.

In August 1991, the joint investigative unit developed a list of 29 CIA employees for priority scrutiny. Ames was at the top of the list.

Yet the first letters to go out to financial institutions requesting access to Ames's financial records did not go out until June 1992, almost 10 months later.

In August 1992, when investigators correlated the records of Ames's bank deposits with what was known about Ames's 1985 meetings at the Soviet Embassy, the joint investigative unit suspected they had their man. When they learned in October of Ames's Swiss bank accounts, their suspicions were confirmed.

But according to the Inspector General's report, this crucial information was not presented to FBI headquarters until January 1993. It was explained to the Committee that the joint investigative unit was looking at possible suspects in addition to Ames. But this still does not explain why significant information pertaining to Ames was not passed contemporaneously to the FBI, particularly given the presence of two FBI agents on the joint investigative unit.

On the basis of the work of the joint investigative unit—which culminated in the March 1993 Skylight/playactor report—the FBI assembled an investigative team and tasked the team members to acquaint themselves with the facts. The FBI began an intensive investigation of Ames shortly thereafter. The Committee was advised in the course of its investigation that FBI headquarters had determined that the earlier information developed on Ames by the joint investigative unit did not meet the standards for an intensive FBI investigation. The Committee believes, however, that there was ample evidence by October 1992, to reasonably suggest that Ames was acting in 1985 (and thereafter) as an agent of the Soviet Union. The FBI's hesitation resulted in a six-month delay before the FBI began to apply the full array of its investigative capabilities against Ames. Once applied, they produced impressive results. Indeed, the FBI investigative team from the Washington

Metropolitan Field Office, together with the CIA, did a superb job in bringing the investigation to a successful conclusion.

Recommendation No. 12: The Director of the FBI should ensure that adequate resources are applied to counterintelligence cases involving the CIA and other federal agencies, and that FBI headquarters is apprised immediately of significant case developments which could form the basis for the FBI's opening an intensive counterintelligence investigation.

Recommendation No. 13: The Attorney General and the Director of the FBI should review the FBI's guidelines for the conduct of counterintelligence investigations to determine whether clearer guidance is needed in determining whether a subject of a counterintelligence inquiry is acting as an agent of a foreign power.

FAILURE TO RESTRICT THE ASSIGNMENTS AND ACCESS TO SUSPECTS IN COUNTERINTELLIGENCE CASES

The Ames case reveals glaring weaknesses in the CIA's procedures for dealing with the career assignments of employees who are under suspicion for compromising intelligence operations. The CIA failed to restrict Ames's assignments and access even after information surfaced in 1989 which indicated Ames was a possible counterintelligence problem.

In September 1989, after a poor tour in Rome, which was known to the managers in the SE Division, his SE superiors allowed Ames to return to the SE Division and assigned him to the office supporting to all Soviet and East European operations in Europe, a position affording him broad access to sensitive information. He remained assigned to the SE Division until August 1990. During this period, investigators learned about Ames's unexplained affluence and developed information regarding several large bank deposits and a particularly large currency exchange. Yet none of this appears to have had any bearing on Ames's continued assignment or access during this period.

In fact, at the end of this assignment, notwithstanding his own poor performance record (he was then ranked 3rd from the bottom among 200 officers in his rating group), Ames was appointed to serve on a promotion board for mid-level CIA operations officers. This assignment gave him access to the personnel records of an entire class of mid-level CIA operations officers.

In October 1990, SE Division managers reassigned Ames to the Counterintelligence Center (CIC) because he had performed poorly and they wanted him out of the Division. Apparently, supervisors in the CIC knew Ames was a poor performer and were aware that questions had been raised about his unexplained affluence. Yet they believed they could manage the problem. After his arrest, these officials recognized that Ames' position had given him access to data which identified virtually every double agent operation controlled by the United States. It is unclear how or why this access was permitted. It is clear that despite the security concerns raised about Ames, his CIC supervisors did not ascertain or evaluate the extent of his access at the time.

In April 1991, while Ames was assigned to the CIC, the Office of Security carried out an updated background investigation of Ames. The results of this investigation were evaluated and shared with the investigator assigned to the special task force. Reflecting interviews with his co-workers in Rome and his Arlington, Virginia neighbors, the investigation produced information that Ames had frequent contacts in Rome with Soviet and

East European officials not fully explained by his work requirements, frequently violated security regulations by leaving his safe open and doing classified work at home, and lived far beyond his CIA salary in both Rome and Arlington. (One of those interviewed went so far as to say that he would not be surprised if Ames were a spy.)

Inexplicably, the CIA security officer who reviewed the investigative report evaluated it as "raising no CI concerns," and the task force investigator assigned to the case did not regard the report as providing any new information. Ames retained his security clearance and his job in the Counterintelligence Center, and no further action was taken to follow-up on the information developed in this report. Indeed, the special task force members viewed the investigative report, together with the favorable results of the April 1991, polygraph, as giving Ames "a clean bill of health."

In September 1991, despite having been "booted out" of the SE Division a year earlier, and despite the special task force inquiry then underway, Ames was allowed to return to the SE Division to conduct a special study of the KGB. While the study itself did not call for particularly sensitive access, Ames once again was given access to the personnel and records of the SE Division.

In December 1991, he was assigned to the Counternarcotics Center (CNC) where he remained until his arrest in 1994. This apparently was the first assignment made on the basis of the security concerns about Ames. But due to the sensitivity of the investigation into the 1985–86 compromises, CNC senior managers were not told of the investigation or the suspicions about Ames until the beginning of the FBI's intensive investigation in 1993. Even then, there was little or no effort made to evaluate and control the extent of Ames' access to classified information. Indeed, investigators later learned that Ames had computer access to a vast range of classified information that did not pertain to counternarcotics. Moreover, when a computer upgrade was installed in November 1993, it provided Ames with the capability to "download" vast quantities of information onto computer discs which he could take out of the building. Fortunately, Ames was arrested before he was able to pass these discs to his KGB handlers. But the fact that he was provided this capability at all at a time when his arrest was imminent is indicative of the CIA's lack of attention to this security problem.

Recommendation No. 14: The Director of Central Intelligence should establish procedures to inform current and prospective supervisors about employees under suspicion in counterintelligence cases. While the need to protect the secrecy of the investigation is essential, as well as the need to protect the employees themselves from unfair personnel actions, the assignment of employees under suspicion without frank consultations at the supervisory level increases the likelihood of serious compromises and leads to conflict between CIA elements.

Recommendation No. 15: The Director of Central Intelligence should issue procedures to require, in any case in which an employee is under suspicion for espionage or related activities, that a systematic evaluation be made of the employee's access to classified information, and that appropriate and timely actions be taken to limit such access. While care must obviously be taken to ensure that such actions do not tip off the employee that he or she is under suspicion, the failure to evaluate the access of an employee in these circumstances may eventually result in damage that might have been prevented.

Recommendation No. 16: The Director of Central Intelligence should establish more stringent criteria for CIA employees serving on promotion and assignment boards, which,

among other things, prevent the appointment to such panels of employees with poor performance records or records of suitability problems.

DEFICIENCIES IN SECURITY PROCEDURES

The Ames case demonstrated numerous deficiencies in the CIA's use of the polygraph, its control over classified documents and materials, and its coordination of security and counterintelligence functions.

THE POLYGRAPH

Ames was able to pass polygraph examinations in 1986 and 1991 with relative ease. Although deeply involved in espionage activities, he was able to answer questions such as whether he worked for a foreign intelligence service, or had contacts with foreign nationals which he failed to report, without showing signs of deception.

The CIA Inspector General's report faults the 1986 examination, finding that the examiner was "too chummy" with Ames. When Ames showed a slight reaction to a question asking whether he had ever been "pitched," i.e., asked to work for a foreign intelligence service, the examiner appeared to readily accept his explanation that he was concerned about being "pitched" in his upcoming assignment in Rome.

The 1991 polygraph examination, according to the Inspector General's report, was deficient in that the examiners (there were two separate sessions) were not sufficiently familiar with the existing information on Ames' unexplained affluence, or with the information developed in the April 1991, background investigation of Ames. The examination was also deficient in that the investigator assigned to the special task force had not participated directly in the examination process, and there had been no prior planning in terms of how the CIA would handle the situation if Ames suddenly made damaging admissions.

According to Ames's debriefings, he did not take drugs or use any particular technique to pass the polygraph examinations. Acting on the advice of the KGB, he tried only to be cooperative and stay as calm as he could. Since he was acquainted with how polygraph examinations were conducted, he also was able to manipulate the process to prevent a "problem" from arising.

If Ames's account is true, it seems to indicate problems beyond those cited by the Inspector General's report, i.e. that examiners should be better informed and prepared. Indeed, it suggests that the CIA's reliance on the results of polygraph examinations needs to be far more circumspect than in the past.

Recommendation No. 17: The Director of Central Intelligence should tighten polygraph procedures to make the polygraph more useful. Such procedures should include random examinations instead of exams at regular intervals, with little or no prior notice, and variations in the polygraph technique. These procedures should also ensure that polygraph examinations involving employees under suspicion are carefully planned and constructed, and that appropriate prior notification is made to the Federal Bureau of Investigation if such cases have potential criminal implications. In addition, the Director should review the policies applicable to the training, supervision, and performance appraisal of polygraph examiners to ensure that polygraph examinations are conducted in a professional manner and produce optimum results.

Recommendation No. 18: The Director of Central Intelligence should institute a fundamental reevaluation of the polygraph as a part of CIA's security program. As the Ames case demonstrates, the polygraph cannot be relied upon with certainty to detect deception. This necessarily puts far more reliance on other aspects of the security process, e.g., background investigations, supervisory reporting, psychological testing, financial reporting, etc. The DCI's review should also include a reevaluation of the use of inconclusive polygraph test results. Even where the polygraph does indicate deception, such information is often useless unless damaging admissions are also obtained from the subject. The Committee believes that if an employee with access to particularly sensitive information does not make such admissions but continues to show deception to relevant questions after adequate testing, there should be additional investigation of the issues in question to attempt to resolve them. Should such investigation fail to do so, the CIA should have the latitude, without prejudice to the employee, to reassign him or her to less sensitive duties.

CONTROL OF CLASSIFIED DOCUMENTS AND MATERIALS

The Ames case also demonstrated gaps in the control of sensitive classified information. Ames was able—without detection—to walk out of CIA headquarters and the U.S. Embassy in Rome with bags and envelopes stuffed with classified documents and materials. Many of the classified documents he passed to his KGB handlers were copies of documents that were not under any system of accountability. Ames did not even have to make copies of them. In his last job in the Counternarcotics Center at the CIA, Ames was able to "download" a variety of classified documents onto computer discs and then simply remove them to his home. When he attended a conference in Turkey in 1993, he brought a lap-top computer to do work in his hotel room. This apparently raised no security concern among those familiar with the incident. He was also able to visit offices he had no reason to be in, and gain access to information he had no business seeing.

In the late 1970s, the CIA instituted a policy calling for random and unannounced spot-checks of personnel leaving Agency compounds. But the policy was discontinued soon thereafter due to the inconvenience caused to those subject to such searches.

Ames recounted later that his KGB handlers were amazed at his ability to gain access to sensitive operations and take large bundles of classified information out of CIA offices without arousing suspicion, a sad commentary on the laxness of security at the CIA.

Recommendation No. 19: The Director of Central Intelligence should reinstate the policy making persons leaving CIA facilities subject to random searches of their person and possessions, and require that such searches be conducted unannounced and periodically at selected locations. Such searches should be conducted frequently enough to serve as a deterrent without unduly hampering the operation of the facilities involved.

Recommendation No. 20: The Director of Central Intelligence should institute computer security measures to prevent employees from being able to "download" classified information onto computer diskettes and removing them from CIA facilities. In addition, existing policies for the introduction, accountability, dissemination, removal, and destruction of all forms of electronic media should be reevaluated. The ability of the CIA's security managers to "audit" specific computer-related functions in order to detect and monitor the actions of suspected offenders should be upgraded.

Recommendation No 21: The Director of Central Intelligence should institute a policy requiring employees to report to their supervisor any instance in which a CIA employee

attempts to obtain classified information which the CIA employee has no apparent reason to know. In turn, supervisors should be required to report to the CIA Counterintelligence Center any such case where a plausible explanation for such a request cannot be ascertained by the supervisor.

Recommendation No. 22: The Director of Central Intelligence should institute new policies to improve the control of classified documents and materials within the CIA. In particular, the Directorate of Operations should undertake an immediate and comprehensive review of its practices and procedures for compartmenting information relating to clandestine operations to ensure that only those officers who absolutely need access can obtain such information. Further, the Directorate should establish and maintain a detailed, automated record of the access granted to each of its employees.

COORDINATION OF SECURITY AND COUNTERINTELLIGENCE

The Ames case demonstrated a serious division between security and counterintelligence activities in the CIA. Even though an investigator from the Office of Security (OS) participated in the investigation of the 1985–86 compromises under the auspices of the Counterintelligence Center (CIC), he failed to coordinate properly with OS with respect to Ames' 1991 polygraph examination. OS had initiated a background investigation of Ames in March 1991, but went ahead with the polygraph in April without the benefit of the background investigation. As it turned out, the background investigation provided significant information about Ames that was largely ignored by the investigator assigned to the CIC in light of Ames's passing the polygraph examination.

Citing senior security officials, the Inspector General's report noted there had always been a "fault line" in communications between the CIC and its predecessors, and the OS. The CIC had not always shared information regarding its counterintelligence investigations and had failed to make use of OS's investigative expertise. Indeed, the search to find the cause of the 1985 compromises might have moved more quickly from analysis to investigation if there had been better coordination between security and counterintelligence.

The Inspector General's report also found "a gradual degradation" of the resources and authority given the security function since 1985, concluding that "this degradation has adversely affected the Agency's ability to prevent and deter activities such as those engaged in by Ames. . . ." The Committee shares the view that this decline has been too great too precipitous. The Committee had recommended an increase in personnel security funding for the CIA and other agencies for Fiscal Year 1995, but was unable to sustain its initiative due to the lack of interest shown by the agencies involved.

Responding to the continuing problem of CIA offices failing to share pertinent information on CIA personnel with one another, Director Woolsey recently created a new Office of Personnel Security that combines elements of the old Office of Personnel, the Office of Medical Services, and the Office of Security. While this consolidation may facilitate the sharing of information regarding suitability problems, it may also hamper the exchange of counterintelligence information from the CIC and may further dilute the security function, particularly the expertise of security investigators.

The Committee believes that the personnel security function should be preserved with a separate office. Routine monitoring of Agency employees from a security perspective remains an important function and one that must be accomplished without carrying a presumption that persons are under suspicion. An effective personnel security program

would deter potential traitors, limit the burden on counterintelligence investigators and result in faster, more effective counterintelligence investigations.

Recommendation No. 23: The Director of Central Intelligence should reexamine the decision to combine the Office of Security with the other elements of the CIA's new personnel center, and should ensure sufficient funding is provided to the personnel security function in Fiscal Year 1995 and in future years. The Director should also clarify the relationship between security and counterintelligence, specifying their respective functions and providing for effective coordination and cooperation between them.

FAILURE TO ADVISE THE OVERSIGHT COMMITTEES

The CIA failed to notify the congressional oversight committees in any meaningful way of the compromises of 1985–1986, as required by applicable law.

Indeed, in the hearings held annually on counterintelligence matters and in numerous staff briefings on the subject from 1985 until 1994, the massive compromises of 1985–86 were never once mentioned by representatives of the CIA or the FBI.

Based upon the recollections of individuals, there were two occasions when the 1985–86 compromises were alluded to in discussions with Members or staff of the Senate Select Committee on Intelligence (SSCI). The first mention came during a staff visit to Moscow in December 1988. The second occurred in 1992 during a visit to Moscow by two Members of the Committee. But on each occasion, the information provided was fragmentary and anecdotal and did not specifically address what was being done by the CIA about the problem. Informal staff efforts to follow-up on each of these conversations were put off by the CIA.

The Committee strongly believes that both the CIA and the FBI had an obligation to advise the oversight committees at the time of the 1985–86 compromises. Section 502 of the National Security Act of 1947 specifically requires intelligence agencies to report to the oversight committees "any significant intelligence failure." The compromises of 1985–86 resulted in a virtual collapse of CIA's Soviet operations at the height of the Cold War. According to the SE Division officer's memorandum of November, 1986, the evidence was at that point "overwhelming" and clearly indicated a problem of disastrous proportions. The oversight committees were responsible for funding the activities of the Directorate of Operations. They should have been formally notified pursuant to section 502 of the National Security Act of 1947.

THE NEED FOR CONTINUED FOLLOW-UP

Many of the problems identified by the Committee are deep-seated and pervasive, and will not be solved easily or quickly. Yet these problems are too important and too integral to the functioning of an agency with important national security responsibilities not to merit continuing and intensive scrutiny by both CIA managers and the congressional oversight committees.

While the Committee intends to make the CIA's response to this report an area of "special oversight interest" in the years ahead, the Committee also directs the Inspector General of the CIA to provide the Committee, through the Director of Central Intelligence, with a report no later than September 1, 1995, and annually thereafter, on the CIA's progress in responding to the recommendations contained in this report and to the continuing counterintelligence and security challenges that the CIA faces.

APPENDIX D

COUNTERTERRORISM, INTELLIGENCE, AND THE HART-RUDMAN COMMISSION, MARCH 2001

Editor's note: Former Senators Gary Hart (D-CO) and Warren Rudman (R-NH) led a Department of Defense study in the months before the 9/11 attacks that concluded the United States was vulnerable to just such a calamity. Reproduced here are the Commission's central thoughts on intelligence reform to strengthen America's antiterrorist stance.

ROAD MAP FOR NATIONAL SECURITY: IMPERATIVE FOR CHANGE

THE PHASE III REPORT OF THE U.S. COMMISSION ON NATIONAL SECURITY/21ST CENTURY MARCH 15, 2001

F. The Intelligence Community

The basic structure of the U.S. intelligence community does not require change. The community has implemented many of the recommendations for reform made by other studies. This Commission's focus is on those changes in intelligence policy, operations, and resources needed for the full implementation of recommendations found elsewhere within this report.

While the intelligence community is generally given high marks for timely and useful contributions to policymaking and crisis management, it failed to warn of Indian nuclear tests or to anticipate the rapidity of missile developments in Iran and North Korea. U.S.

Source: *Road Map for National Security: Imperative for Change*, U.S. Commission on National Security/21st Century (the Hart-Rudman Commission), Phase III Report (March 15, 2001), pp. 82–86.

intelligence has, at times, been unable to respond to the burgeoning requirements levied by more demanding consumers trying to cope with a more complex array of problems. Steep declines in human intelligence resources over the last decade have been forcing dangerous tradeoffs between coverage of important countries, regions, and functional challenges. Warfighters in theater are often frustrated because the granulated detail of intelligence that they need rarely gets to them, even though they know that it exists somewhere in the intelligence system.

It is a commonplace that the intelligence community lost its focus when the Berlin Wall fell. Since then, three other problems have compounded its challenges. First, the world is a more complex place, with more diffuse dangers requiring different kinds of intelligence and new means of acquiring them. Second, its resources—personnel and monetary—have been reduced. Third, the dangers of terrorism and proliferation, as well as ethnic conflicts and humanitarian emergencies, have led to a focus on providing warning and crisis management rather than long-term analysis.

The result of these three developments is an intelligence community that is more demand-driven than it was two decades ago. That demand is also more driven by military consumers and, therefore, what the intelligence community is doing is narrower and more short-term than it was two decades ago. Given the paucity of resources, this means that important regions and trends are not receiving adequate attention and that the more comprehensive analytical tasks that everyone agrees the intelligence community should be performing simply cannot be done properly.

This Commission has emphasized that *strategic planning* needs to be introduced throughout the national security institutions of the U.S. government. We have also emphasized the critical importance of *preventive diplomac*y. Both require an intelligence community that can support such innovations, *but current trends are leading in the opposite direction.*

This Commission has also stressed the increasing importance of diplomatic and especially economic components in U.S. statecraft. The intelligence community as a whole needs to maintain its level of effort in military domains, but also to do much more in economic domains. In a world where proprietary science and technology developments are increasingly the sinews of national power, the intelligence community needs to be concerned more than ever with U.S. technological security, not least in cyberspace. And here, too, the trends within the intelligence community point not toward, but away from, the country's essential needs. Resources devoted to handling such economic and technical issues are not increasing, but declining.

To respond to these challenges, some recommend strengthening the Director of Central Intelligence (DCI) through organizational changes, such as vesting greater budgetary authority in him and giving him greater control over community personnel. We believe, however, that current efforts to strengthen community management while maintaining the ongoing relationship between the DCI and the Secretary of Defense are bearing fruit. We recommend no major structural changes, but offer certain recommendations to strengthen the DCI's role and the efficiency of the process.

The National Security Act of 1947 gave the National Security Council responsibility for providing guidance with respect to intelligence functions. In practice, however, administrations have varied widely in their approach to this function—sometimes actively setting priorities for intelligence collection and analysis and sometimes focusing simply on coordinating intelligence response in times of crisis.

To achieve the strategy envisioned in our Phase II report, and to make the budgetary recommendations of this section most effective, more consistent attention must be paid to the setting of national intelligence priorities. To do this, we recommend the following:

36 The President should order the setting of national intelligence priorities through National Security Council guidance to the Director of Central Intelligence.

In recommending this, we echo the conclusion of the Commission on the Roles and Capabilities of the United States Intelligence Community (the Brown-Rudman Commission). While we do not want to dictate how future Presidents might use the National Security Council, we believe this is a crucial function that must be filled in some way. The President's authority to set strategic intelligence priorities should be exercised through continuous NSC engagement with the DCI, from which the DCI can establish appropriate collection and analysis priorities. Such an approach would ensure consistent policymaker input into the intelligence effort and, if policymakers come to feel a part of the intelligence process, it should enable greater support for the intelligence community, as well. We believe that this function would be best fulfilled by a true strategic planning staff at the NSC—as discussed in our recommendation 14. *The point is that policy and strategic guidance for intelligence should be formulated in tandem.*

We have emphasized the importance of securing the homeland in this new century and have urged, specifically in recommendation 4, that it be a higher intelligence priority. Making it so means greatly strengthening U.S. human intelligence (HUMINT) capability. This involves ensuring the quality of those entering the community's clandestine service, as well as the recruitment of foreign nationals as agents with the best chance of providing crucial information about terrorism and other threats to the homeland.

Along with the National Commission on Terrorism, we believe that guidelines for the recruitment of foreign nationals should be reviewed to ensure that, while respecting legal and human rights concerns, they maximize the intelligence community's ability to collect intelligence on terrorist plans and methods. We recognize the need to observe basic moral standards in all U.S. government conduct, but the people who can best help U.S. agents penetrate effectively into terrorist organizations, for example, are not liable to be model citizens of spotless virtue. Operative regulations in this respect must balance national security interests with concern for American values and principles. We therefore recommend the following:

37 The Director of Central Intelligence should emphasize the recruitment of human intelligence sources on terrorism as one of the intelligence community's highest priorities, and ensure that operational guidelines are balanced between security needs and respect for American values and principles.

The DCI must also give greater priority to the analysis of economic and science and technology trends where the U.S. intelligence community's capabilities are inadequate. While improvements have been made, especially in the wake of the Asian financial crisis, the global economic and scientific environments are changing so rapidly and dramatically that the United States needs to develop new tools merely to understand what is happening in the world. The Treasury Department has made important strides in this regard, but it has a

long way to go. Treasury and CIA also need to coordinate better efforts in this critical area. We therefore recommend the following:

38 The intelligence community should place new emphasis on collection and analysis of economic and science/technology security concerns, and incorporate more open-source intelligence into analytical products. Congress should support this new emphasis by increasing significantly the National Foreign Intelligence Program (NFIP) budget for collection and analysis.

In order to maintain U.S. strength in traditional areas while building new capabilities, the President and the Congress should give priority to economic and science/technology intelligence. We need to increase overall funding in these areas significantly and the DCI needs to emphasize improvement in the collection and analysis of this intelligence. This will require, in turn, a major investment in the community's long-term analytical capacities, but these capacities are crucial in any event to supporting the strategic planning that we have emphasized throughout this report.

Better analysis in non-military areas also means ensuring that open-source intelligence is a vital part of all-source analysis. Many new challenges, but especially economic, scientific, and technological ones, call for greater attention to the wealth of openly available information. Analyses of the failure of the community to anticipate India's nuclear tests, when clear indications were available in open-source publications, demonstrate that this capability has relevance for traditional security issues as well.

We thus urge the strengthening of HUMINT capabilities, the broadening of analytical efforts across a range of issues, and the incorporation of more open-source information into all-source analysis. Meeting the nation's future intelligence needs, however, will also require changes in the community's technological capabilities.

Technological superiority has long been a hallmark of U.S. intelligence. Yet some agencies within the National Foreign Intelligence Program spend as little as three to four percent of their budget on all aspects of research and development, and as little as one percent on advanced research and development. This reflects a decline in overall intelligence expenditures in real terms, while salaries and benefits for intelligence personnel have been on the rise. Concerted effort is needed to ensure that research and development receive greater funding.

At the same time, the intelligence community must think about its technological capabilities in new ways. During the Cold War, the National Security Agency (NSA) and other agencies derived a great wealth of information through signals and communications intelligence. In today's Internet age, global networks, cable, and wireless communications are increasingly ubiquitous, with attendant improvements in encryption technologies. Together these trends make signal intelligence collection increasingly difficult. The United States must possess the best platforms and capabilities to ensure that it can collect necessary information consistent with respecting Americans' privacy. It must also have high-quality technical and scientific personnel able to respond to future challenges.

To achieve these ends, ***we recommend that the DCI should provide the President a strategic assessment of the effectiveness of current technical intelligence capabilities to ensure the fullest range of collection across all intelligence domains, particularly as they relate to cyberspace and new communications technologies.***

Should the U.S. intelligence community lack a full-spectrum capability either in collection or analysis, the United States would forfeit the depth of intelligence coverage

it enjoyed during the Cold War. Maintaining this edge will require greater funding and expertise in the information and communication sciences. We must also pursue innovative approaches with the private sector to establish access to new technologies as they become available.

This Commission, in sum, urges an overall increase in the NFIP budget to accommodate greater priority placed on nonmilitary intelligence challenges. Military intelligence needs also remain critical, however, so a simple reallocation of existing resources will not suffice. To ensure the continuing technological strength of the community, and to build cutting-edge intelligence platforms, there is no escaping the need for an increase in overall resources for the intelligence community.

APPENDIX E

THE 9/11 COMMISSION RECOMMENDATIONS ON INTELLIGENCE AND COUNTERTERRORISM, 2004

Editor's note: The 9/11 or Kean Commission (led by Republican former governor of New Jersey, Thomas H. Kean) reported in 2004 on its findings regarding the Al Qaeda terrorist attacks against the United States on September 11, 2001. Following are the Commission's main findings on how to organize the government differently to deal with the terrorist threat.

12 WHAT TO DO? A GLOBAL STRATEGY

12.1 REFLECTING ON A GENERATIONAL CHALLENGE

Three years after 9/11, Americans are still thinking and talking about how to protect our nation in this new era. The national debate continues.

Countering terrorism has become, beyond any doubt, the top national security priority for the United States. This shift has occurred with the full support of the Congress, both major political parties, the media, and the American people.

The nation has committed enormous resources to national security and to countering terrorism. Between fiscal year 2001, the last budget adopted before 9/11, and the present fiscal year 2004, total federal spending on defense (including expenditures on both Iraq and Afghanistan), homeland security, and international affairs rose more than 50 percent, from $354 billion to about $547 billion. The United States has not experienced such a rapid surge in national security spending since the Korean War.[1]

This pattern has occurred before in American history. The United States faces a sudden crisis and summons a tremendous exertion of national energy. Then, as that surge

---

Source: *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W.W. Norton, 2004), pp. 361–428, 562–67.

transforms the landscape, comes a time for reflection and reevaluation. Some programs and even agencies are discarded; others are invented or redesigned. Private firms and engaged citizens redefine their relationships with government, working through the processes of the American republic.

Now is the time for that reflection and reevaluation. The United States should consider *what to do*—the shape and objectives of a strategy. Americans should also consider *how to do it*—organizing their government in a different way.

Defining the Threat

In the post-9/11 world, threats are defined more by the fault lines within societies than by the territorial boundaries between them. From terrorism to global disease or environmental degradation, the challenges have become transnational rather than international. That is the defining quality of world politics in the twenty-first century.

National security used to be considered by studying foreign frontiers, weighing opposing groups of states, and measuring industrial might. To be dangerous, an enemy had to muster large armies. Threats emerged slowly, often visibly, as weapons were forged, armies conscripted, and units trained and moved into place. Because large states were more powerful, they also had more to lose. They could be deterred.

Now threats can emerge quickly. An organization like al Qaeda, headquartered in a country on the other side of the earth, in a region so poor that electricity or telephones were scarce, could nonetheless scheme to wield weapons of unprecedented destructive power in the largest cities of the United States.

In this sense, 9/11 has taught us that terrorism against American interests "over there" should be regarded just as we regard terrorism against America "over here." In this same sense, the American homeland is the planet.

But the enemy is not just "terrorism," some generic evil.[2] This vagueness blurs the strategy. The catastrophic threat at this moment in history is more specific. It is the threat posed by *Islamist* terrorism—especially the al Qaeda network, its affiliates, and its ideology.[3]

As we mentioned in chapter 2, Usama Bin Ladin and other Islamist terrorist leaders draw on a long tradition of extreme intolerance within one stream of Islam (a minority tradition), from at least Ibn Taimiyyah, through the founders of Wahhabism, through the Muslim Brotherhood, to Sayyid Qutb. That stream is motivated by religion and does not distinguish politics from religion, thus distorting both. It is further fed by grievances stressed by Bin Ladin and widely felt throughout the Muslim world—against the U.S. military presence in the Middle East, policies perceived as anti-Arab and anti-Muslim, and support of Israel. Bin Ladin and Islamist terrorists mean exactly what they say: to them America is the font of all evil, the "head of the snake," and it must be converted or destroyed.

It is not a position with which Americans can bargain or negotiate. With it there is no common ground—not even respect for life—on which to begin a dialogue. It can only be destroyed or utterly isolated.

Because the Muslim world has fallen behind the West politically, economically, and militarily for the past three centuries, and because few tolerant or secular Muslim democracies provide alternative models for the future, Bin Ladin's message finds receptive ears. It has attracted active support from thousands of disaffected young Muslims and

resonates powerfully with a far larger number who do not actively support his methods. The resentment of America and the West is deep, even among leaders of relatively successful Muslim states.[4]

Tolerance, the rule of law, political and economic openness, the extension of greater opportunities to women—these cures must come from within Muslim societies themselves. The United States must support such developments.

But this process is likely to be measured in decades, not years. It is a process that will be violently opposed by Islamist terrorist organizations, both inside Muslim countries and in attacks on the United States and other Western nations. The United States finds itself caught up in a clash *within* a civilization. That clash arises from particular conditions in the Muslim world, conditions that spill over into expatriate Muslim communities in non-Muslim countries.

Our enemy is twofold: al Qaeda, a stateless network of terrorists that struck us on 9/11; and a radical ideological movement in the Islamic world, inspired in part by al Qaeda, which has spawned terrorist groups and violence across the globe. The first enemy is weakened, but continues to pose a grave threat. The second enemy is gathering, and will menace Americans and American interests long after Usama Bin Ladin and his cohorts are killed or captured. Thus our strategy must match our means to two ends: dismantling the al Qaeda network and prevailing in the longer term over the ideology that gives rise to Islamist terrorism.

Islam is not the enemy. It is not synonymous with terror. Nor does Islam teach terror. America and its friends oppose a perversion of Islam, not the great world faith itself. Lives guided by religious faith, including literal beliefs in holy scriptures, are common to every religion, and represent no threat to us.

Other religions have experienced violent internal struggles. With so many diverse adherents, every major religion will spawn violent zealots. Yet understanding and tolerance among people of different faiths can and must prevail.

The present transnational danger is Islamist terrorism. What is needed is a broad political-military strategy that rests on a firm tripod of policies to

- attack terrorists and their organizations;
- prevent the continued growth of Islamist terrorism; and
- protect against and prepare for terrorist attacks.

More Than a War on Terrorism

Terrorism is a tactic used by individuals and organizations to kill and destroy. Our efforts should be directed at those individuals and organizations.

Calling this struggle a war accurately describes the use of American and allied armed forces to find and destroy terrorist groups and their allies in the field, notably in Afghanistan. The language of war also evokes the mobilization for a national effort. Yet the strategy should be balanced.

The first phase of our post-9/11 efforts rightly included military action to topple the Taliban and pursue al Qaeda. This work continues. But long-term success demands the use of all elements of national power: diplomacy, intelligence, covert action, law enforcement, economic policy, foreign aid, public diplomacy, and homeland defense. If we favor one tool while neglecting others, we leave ourselves vulnerable and weaken our national effort.

Certainly the strategy should include offensive operations to counter terrorism. Terrorists should no longer find safe haven where their organizations can grow and flourish. America's strategy should be a coalition strategy, that includes Muslim nations as partners in its development and implementation.

Our effort should be accompanied by a preventive strategy that is as much, or more, political as it is military. The strategy must focus clearly on the Arab and Muslim world, in all its variety.

Our strategy should also include defenses. America can be attacked in many ways and has many vulnerabilities. No defenses are perfect. But risks must be calculated; hard choices must be made about allocating resources. Responsibilities for America's defense should be clearly defined. Planning does make a difference, identifying where a little money might have a large effect. Defenses also complicate the plans of attackers, increasing their risks of discovery and failure. Finally, the nation must prepare to deal with attacks that are not stopped.

Measuring Success

What should Americans expect from their government in the struggle against Islamist terrorism? The goals seem unlimited: Defeat terrorism anywhere in the world. But Americans have also been told to expect the worst: An attack is probably coming; it may be terrible.

With such benchmarks, the justifications for action and spending seem limitless. Goals are good. Yet effective public policies also need concrete objectives. Agencies need to be able to measure success.

These measurements do not need to be quantitative: government cannot measure success in the ways that private firms can. But the targets should be specific enough so that reasonable observers—in the White House, the Congress, the media, or the general public—can judge whether or not the objectives have been attained.

Vague goals match an amorphous picture of the enemy. Al Qaeda and its affiliates are popularly described as being all over the world, adaptable, resilient, needing little higher-level organization, and capable of anything. The American people are thus given the picture of an omnipotent, unslayable hydra of destruction. This image lowers expectations for government effectiveness.

It should not lower them too far. Our report shows a determined and capable group of plotters. Yet the group was fragile, dependent on a few key personalities, and occasionally left vulnerable by the marginal, unstable people often attracted to such causes. The enemy made mistakes—like Khalid al Mihdhar's unauthorized departure from the United States that required him to enter the country again in July 2001, or the selection of Zacarias Moussaoui as a participant and Ramzi Binalshibh's transfer of money to him. The U.S. government was not able to capitalize on those mistakes in time to prevent 9/11.

We do not believe it is possible to defeat all terrorist attacks against Americans, every time and everywhere. A president should tell the American people:

- No president can promise that a catastrophic attack like that of 9/11 will not happen again. History has shown that even the most vigilant and expert agencies cannot always prevent determined, suicidal attackers from reaching a target.

- But the American people are entitled to expect their government to do its very best. They should expect that officials will have realistic objectives, clear guidance, and effective organization. They are entitled to see some standards for performance so they can judge, with the help of their elected representatives, whether the objectives are being met.

12.2 ATTACK TERRORISTS AND THEIR ORGANIZATIONS

The U.S. government, joined by other governments around the world, is working through intelligence, law enforcement, military, financial, and diplomatic channels to identify, disrupt, capture, or kill individual terrorists. This effort was going on before 9/11 and it continues on a vastly enlarged scale. But to catch terrorists, a U.S. or foreign agency needs to be able to find and reach them.

No Sanctuaries

The 9/11 attack was a complex international operation, the product of years of planning. Bombings like those in Bali in 2003 or Madrid in 2004, while able to take hundreds of lives, can be mounted locally. Their requirements are far more modest in size and complexity. They are more difficult to thwart. But the U.S. government must build the capacities to prevent a 9/11-scale plot from succeeding, and those capabilities will help greatly to cope with lesser but still devastating attacks.

A complex international terrorist operation aimed at launching a catastrophic attack cannot be mounted by just anyone in any place. Such operations appear to require

- time, space, and ability to perform competent planning and staff work;
- a command structure able to make necessary decisions and possessing the authority and contacts to assemble needed people, money, and materials;
- opportunity and space to recruit, train, and select operatives with the needed skills and dedication, providing the time and structure required to socialize them into the terrorist cause, judge their trustworthiness, and hone their skills;
- a logistics network able to securely manage the travel of operatives, move money, and transport resources (like explosives) where they need to go;
- access, in the case of certain weapons, to the special materials needed for a nuclear, chemical, radiological, or biological attack;
- reliable communications between coordinators and operatives; and
- opportunity to test the workability of the plan.

Many details in chapters 2, 5, and 7 illustrate the direct and indirect value of the Afghan sanctuary to al Qaeda in preparing the 9/11 attack and other operations. The organization cemented personal ties among veteran jihadists working together there for years. It had the operational space to gather and sift recruits, indoctrinating them in isolated, desert camps. It built up logistical networks, running through Pakistan and the United Arab Emirates.

Al Qaeda also exploited relatively lax internal security environments in Western countries, especially Germany. It considered the environment in the United States so hospitable that the 9/11 operatives used America as their staging area for further training

and exercises—traveling into, out of, and around the country and complacently using their real names with little fear of capture.

To find sanctuary, terrorist organizations have fled to some of the least governed, most lawless places in the world. The intelligence community has prepared a world map that highlights possible terrorist havens, using no secret intelligence—just indicating areas that combine rugged terrain, weak governance, room to hide or receive supplies, and low population density with a town or city near enough to allow necessary interaction with the outside world. Large areas scattered around the world meet these criteria.[5]

In talking with American and foreign government officials and military officers on the front lines fighting terrorists today, we asked them: If you were a terrorist leader today, where would you locate your base? Some of the same places come up again and again on their lists:

- western Pakistan and the Pakistan-Afghanistan border region
- southern or western Afghanistan
- the Arabian Peninsula, especially Saudi Arabia and Yemen, and the nearby Horn of Africa, including Somalia and extending southwest into Kenya
- Southeast Asia, from Thailand to the southern Philippines to Indonesia
- West Africa, including Nigeria and Mali
- European cities with expatriate Muslim communities, especially cities in central and eastern Europe where security forces and border controls are less effective

In the twentieth century, strategists focused on the world's great industrial heartlands. In the twenty-first, the focus is in the opposite direction, toward remote regions and failing states. The United States has had to find ways to extend its reach, straining the limits of its influence.

Every policy decision we make needs to be seen through this lens. If, for example, Iraq becomes a failed state, it will go to the top of the list of places that are breeding grounds for attacks against Americans at home. Similarly, if we are paying insufficient attention to Afghanistan, the rule of the Taliban or warlords and narcotraffickers may reemerge and its countryside could once again offer refuge to al Qaeda, or its successor.

Recommendation: The U.S. government must identify and prioritize actual or potential terrorist sanctuaries. For each, it should have a realistic strategy to keep possible terrorists insecure and on the run, using all elements of national power. We should reach out, listen to, and work with other countries that can help.

We offer three illustrations that are particularly applicable today, in 2004: Pakistan, Afghanistan, and Saudi Arabia.

PAKISTAN

Pakistan's endemic poverty, widespread corruption, and often ineffective government create opportunities for Islamist recruitment. Poor education is a particular concern. Millions of families, especially those with little money, send their children to religious schools, or madrassahs. Many of these schools are the only opportunity available for an education, but some have been used as incubators for violent extremism. According to Karachi's

police commander, there are 859 madrassahs teaching more than 200,000 youngsters in his city alone.[6]

It is hard to overstate the importance of Pakistan in the struggle against Islamist terrorism. Within Pakistan's borders are 150 million Muslims, scores of al Qaeda terrorists, many Taliban fighters, and—perhaps—Usama Bin Ladin. Pakistan possesses nuclear weapons and has come frighteningly close to war with nuclear-armed India over the disputed territory of Kashmir. A political battle among anti-American Islamic fundamentalists, the Pakistani military, and more moderate mainstream political forces has already spilled over into violence, and there have been repeated recent attempts to kill Pakistan's president, Pervez Musharraf.

In recent years, the United States has had three basic problems in its relationship with Pakistan:

- On terrorism, Pakistan helped nurture the Taliban. The Pakistani army and intelligence services, especially below the top ranks, have long been ambivalent about confronting Islamist extremists. Many in the government have sympathized with or provided support to the extremists. Musharraf agreed that Bin Ladin was bad. But before 9/11, preserving good relations with the Taliban took precedence.
- On proliferation, Musharraf has repeatedly said that Pakistan does not barter with its nuclear technology. But proliferation concerns have been long-standing and very serious. Most recently, the Pakistani government has claimed not to have known that one of its nuclear weapons developers, a national figure, was leading the most dangerous nuclear smuggling ring ever disclosed.
- Finally, Pakistan has made little progress toward the return of democratic rule at the national level, although that turbulent process does continue to function at the provincial level and the Pakistani press remains relatively free.

Immediately after 9/11, confronted by the United States with a stark choice, Pakistan made a strategic decision. Its government stood aside and allowed the U.S.-led coalition to destroy the Taliban regime. In other ways, Pakistan actively assisted: its authorities arrested more than 500 al Qaeda operatives and Taliban members, and Pakistani forces played a leading part in tracking down KSM, Abu Zubaydah, and other key al Qaeda figures.[7]

In the following two years, the Pakistani government tried to walk the fence, helping against al Qaeda while seeking to avoid a larger confrontation with Taliban remnants and other Islamic extremists. When al Qaeda and its Pakistani allies repeatedly tried to assassinate Musharraf, almost succeeding, the battle came home.

The country's vast unpoliced regions make Pakistan attractive to extremists seeking refuge and recruits and also provide a base for operations against coalition forces in Afghanistan. Almost all the 9/11 attackers traveled the north-south nexus of Kandahar–Quetta–Karachi. The Baluchistan region of Pakistan (KSM's ethnic home) and the sprawling city of Karachi remain centers of Islamist extremism where the U.S. and Pakistani security and intelligence presence has been weak. The U.S. consulate in Karachi is a makeshift fortress, reflecting the gravity of the surrounding threat.[8]

During the winter of 2003–2004, Musharraf made another strategic decision. He ordered the Pakistani army into the frontier provinces of northwest Pakistan along the Afghan border, where Bin Ladin and Ayman al Zawahiri have reportedly taken refuge. The army is confronting groups of al Qaeda fighters and their local allies in very difficult terrain.

On the other side of the frontier, U.S. forces in Afghanistan have found it challenging to organize effective joint operations, given Pakistan's limited capabilities and reluctance to permit U.S. military operations on its soil. Yet in 2004, it is clear that the Pakistani government is trying harder than ever before in the battle against Islamist terrorists.[9]

Acknowledging these problems and Musharraf's own part in the story, we believe that Musharraf's government represents the best hope for stability in Pakistan and Afghanistan.

- In an extraordinary public essay asking how Muslims can "drag ourselves out of the pit we find ourselves in, to raise ourselves up," Musharraf has called for a strategy of "enlightened moderation." The Muslim world, he said, should shun militancy and extremism; the West—and the United States in particular—should seek to resolve disputes with justice and help better the Muslim world.[10]
- Having come close to war in 2002 and 2003, Pakistan and India have recently made significant progress in peacefully discussing their longstanding differences. The United States has been and should remain a key supporter of that process.
- The constant refrain of Pakistanis is that the United States long treated them as allies of convenience. As the United States makes fresh commitments now, it should make promises it is prepared to keep, for years to come.

Recommendation: If Musharraf stands for enlightened moderation in a fight for his life and for the life of his country, the United States should be willing to make hard choices too, and make the difficult long-term commitment to the future of Pakistan. Sustaining the current scale of aid to Pakistan, the United States should support Pakistan's government in its struggle against extremists with a comprehensive effort that extends from military aid to support for better education, so long as Pakistan's leaders remain willing to make difficult choices of their own.

Afghanistan

Afghanistan was the incubator for al Qaeda and for the 9/11 attacks. In the fall of 2001, the U.S.-led international coalition and its Afghan allies toppled the Taliban and ended the regime's protection of al Qaeda. Notable progress has been made. International cooperation has been strong, with a clear UN mandate and a NATO-led peacekeeping force (the International Security Assistance Force, or ISAF). More than 10,000 American soldiers are deployed today in Afghanistan, joined by soldiers from NATO allies and Muslim states. A central government has been established in Kabul, with a democratic constitution, new currency, and a new army. Most Afghans enjoy greater freedom, women and girls are emerging from subjugation, and 3 million children have returned to school. For the first time in many years, Afghans have reason to hope.[11]

But grave challenges remain. Taliban and al Qaeda fighters have regrouped in the south and southeast. Warlords control much of the country beyond Kabul, and the land is awash in weapons. Economic development remains a distant hope. The narcotics trade—long a massive sector of the Afghan economy—is again booming. Even the most hardened aid workers refuse to operate in many regions, and some warn that Afghanistan is near the brink of chaos.[12]

Battered Afghanistan has a chance. Elections are being prepared. It is revealing that in June 2004,Taliban fighters resorted to slaughtering 16 Afghans on a bus, apparently for no

reason other than their boldness in carrying an unprecedented Afghan weapon: a voter registration card.

Afghanistan's president, Hamid Karzai, is brave and committed. He is trying to build genuinely national institutions that can overcome the tradition of allocating powers among ethnic communities. Yet even if his efforts are successful and elections bring a democratic government to Afghanistan, the United States faces some difficult choices.

After paying relatively little attention to rebuilding Afghanistan during the military campaign, U.S. policies changed noticeably during 2003. Greater consideration of the political dimension and congressional support for a substantial package of assistance signaled a longer-term commitment to Afghanistan's future. One Afghan regional official plaintively told us the country finally has a good government. He begged the United States to keep its promise and not abandon Afghanistan again, as it had in the 1990s. Another Afghan leader noted that if the United States leaves, "we will lose all that we have gained."[13]

Most difficult is to define the security mission in Afghanistan. There is continuing political controversy about whether military operations in Iraq have had any effect on the scale of America's commitment to the future of Afghanistan. The United States has largely stayed out of the central government's struggles with dissident warlords and it has largely avoided confronting the related problem of narcotrafficking.[14]

Recommendation: The President and the Congress deserve praise for their efforts in Afghanistan so far. Now the United States and the international community should make a long-term commitment to a secure and stable Afghanistan, in order to give the government a reasonable opportunity to improve the life of the Afghan people. Afghanistan must not again become a sanctuary for international crime and terrorism. The United States and the international community should help the Afghan government extend its authority over the country, with a strategy and nation-by-nation commitments to achieve their objectives.

- This is an ambitious recommendation. It would mean a redoubled effort to secure the country, disarm militias, and curtail the age of warlord rule. But the United States and NATO have already committed themselves to the future of this region—wisely, as the 9/11 story shows—and failed half-measures could be worse than useless.
- NATO in particular has made Afghanistan a test of the Alliance's ability to adapt to current security challenges of the future. NATO must pass this test. Currently, the United States and the international community envision enough support so that the central government can build a truly national army and extend essential infrastructure and minimum public services to major towns and regions. The effort relies in part on foreign civil-military teams, arranged under various national flags. The institutional commitments of NATO and the United Nations to these enterprises are weak. NATO member states are not following through; some of the other states around the world that have pledged assistance to Afghanistan are not fulfilling their pledges.
- The U.S. presence in Afghanistan is overwhelmingly oriented toward military and security work. The State Department presence is woefully understaffed, and the military mission is narrowly focused on al Qaeda and Taliban remnants in the south and southeast. The U.S. government can do its part if the international community decides on a joint effort to restore the rule of law and contain rampant crime and narcotics trafficking in this crossroads of Central Asia.[15]

We heard again and again that the money for assistance is allocated so rigidly that, on the ground, one U.S. agency often cannot improvise or pitch in to help another agency, even in small ways when a few thousand dollars could make a great difference.

The U.S. government should allocate money so that lower-level officials have more flexibility to get the job done across agency lines, adjusting to the circumstances they find in the field. This should include discretionary funds for expenditures by military units that often encounter opportunities to help the local population.

Saudi Arabia

Saudi Arabia has been a problematic ally in combating Islamic extremism. At the level of high policy, Saudi Arabia's leaders cooperated with American diplomatic initiatives aimed at the Taliban or Pakistan before 9/11. At the same time, Saudi Arabia's society was a place where al Qaeda raised money directly from individuals and through charities. It was the society that produced 15 of the 19 hijackers.

The Kingdom is one of the world's most religiously conservative societies, and its identity is closely bound to its religious links, especially its position as the guardian of Islam's two holiest sites. Charitable giving, or *zakat,* is one of the five pillars of Islam. It is broader and more pervasive than Western ideas of charity—functioning also as a form of income tax, educational assistance, foreign aid, and a source of political influence. The Western notion of the separation of civic and religious duty does not exist in Islamic cultures. Funding charitable works is an integral function of the governments in the Islamic world. It is so ingrained in Islamic culture that in Saudi Arabia, for example, a department within the Saudi Ministry of Finance and National Economy collects zakat directly, much as the U.S. Internal Revenue Service collects payroll withholding tax. Closely tied to zakat is the dedication of the government to propagating the Islamic faith, particularly the Wahhabi sect that flourishes in Saudi Arabia.

Traditionally, throughout the Muslim world, there is no formal oversight mechanism for donations. As Saudi wealth increased, the amounts contributed by individuals and the state grew dramatically. Substantial sums went to finance Islamic charities of every kind.

While Saudi domestic charities are regulated by the Ministry of Labor and Social Welfare, charities and international relief agencies, such as the World Assembly of MuslimYouth (WAMY), are currently regulated by the Ministry of Islamic Affairs. This ministry uses zakat and government funds to spread Wahhabi beliefs throughout the world, including in mosques and schools. Often these schools provide the only education available; even in affluent countries, Saudi-funded Wahhabi schools are often the only Islamic schools. Some Wahhabi-funded organizations have been exploited by extremists to further their goal of violent jihad against non-Muslims. One such organization has been the al Haramain Islamic Foundation; the assets of some branch offices have been frozen by the U.S. and Saudi governments.

Until 9/11, few Saudis would have considered government oversight of charitable donations necessary; many would have perceived it as interference in the exercise of their faith. At the same time, the government's ability to finance most state expenditures with energy revenues has delayed the need for a modern income tax system. As a result, there have been strong religious, cultural, and administrative barriers to monitoring charitable spending. That appears to be changing, however, now that the goal of violent jihad also extends to overthrowing Sunni governments (such as the House of Saud) that are not living up to the ideals of the Islamist extremists.[16]

The leaders of the United States and the rulers of Saudi Arabia have long had friendly relations, rooted in fundamentally common interests against the Soviet Union during the Cold War, in American hopes that Saudi oil supplies would stabilize the supply and price of oil in world markets, and in Saudi hopes that America could help protect the Kingdom against foreign threats.

In 1990, the Kingdom hosted U.S. armed forces before the first U.S.-led war against Iraq. American soldiers and airmen have given their lives to help protect Saudi Arabia. The Saudi government has difficulty acknowledging this. American military bases remained there until 2003, as part of an international commitment to contain Iraq.

For many years, leaders on both sides preferred to keep their ties quiet and behind the scenes. As a result, neither the U.S. nor the Saudi people appreciated all the dimensions of the bilateral relationship, including the Saudi role in U.S. strategies to promote the Middle East peace process. In each country, political figures find it difficult to publicly defend good relations with the other.

Today, mutual recriminations flow. Many Americans see Saudi Arabia as an enemy, not as an embattled ally. They perceive an autocratic government that oppresses women, dominated by a wealthy and indolent elite. Saudi contacts with American politicians are frequently invoked as accusations in partisan political arguments. Americans are often appalled by the intolerance, anti-Semitism, and anti-American arguments taught in schools and preached in mosques.

Saudis are angry too. Many educated Saudis who were sympathetic to America now perceive the United States as an unfriendly state. One Saudi reformer noted to us that the demonization of Saudi Arabia in the U.S. media gives ammunition to radicals, who accuse reformers of being U.S. lackeys. Tens of thousands of Saudis who once regularly traveled to (and often had homes in) the United States now go elsewhere.[17]

Among Saudis, the United States is seen as aligned with Israel in its conflict with the Palestinians, with whom Saudis ardently sympathize. Although Saudi Arabia's cooperation against terrorism improved to some extent after the September 11 attacks, significant problems remained. Many in the Kingdom initially reacted with disbelief and denial. In the following months, as the truth became clear, some leading Saudis quietly acknowledged the problem but still did not see their own regime as threatened, and thus often did not respond promptly to U.S. requests for help. Though Saddam Hussein was widely detested, many Saudis are sympathetic to the anti-U.S. insurgents in Iraq, although majorities also condemn jihadist attacks in the Kingdom.[18]

As in Pakistan, Yemen, and other countries, attitudes changed when the terrorism came home. Cooperation had already become significant, but after the bombings in Riyadh on May 12, 2003, it improved much more. The Kingdom openly discussed the problem of radicalism, criticized the terrorists as religiously deviant, reduced official support for religious activity overseas, closed suspect charitable foundations, and publicized arrests—very public moves for a government that has preferred to keep internal problems quiet.

The Kingdom of Saudi Arabia is now locked in mortal combat with al Qaeda. Saudi police are regularly being killed in shootouts with terrorists. In June 2004, the Saudi ambassador to the United States called publicly—in the Saudi press—for his government to wage a jihad of its own against the terrorists. "We must all, as a state and as a people, recognize the truth about these criminals," he declared, "[i]f we do not declare a general mobilization—we will lose this war on terrorism."[19]

Saudi Arabia is a troubled country. Although regarded as very wealthy, in fact per capita income has dropped from $28,000 at its height to the present level of about $8,000. Social and religious traditions complicate adjustment to modern economic activity and limit employment opportunities for young Saudis. Women find their education and employment sharply limited.

President Clinton offered us a perceptive analysis of Saudi Arabia, contending that fundamentally friendly rulers have been constrained by their desire to preserve the status quo. He, like others, made the case for pragmatic reform instead. He hopes the rulers will envision what they want their Kingdom to become in 10 or 20 years, and start a process in which their friends can help them change.[20]

There are signs that Saudi Arabia's royal family is trying to build a consensus for political reform, though uncertain about how fast and how far to go. Crown Prince Abdullah wants the Kingdom to join the World Trade Organization to accelerate economic liberalization. He has embraced the *Arab Human Development Report*, which was highly critical of the Arab world's political, economic, and social failings and called for greater economic and political reform.[21]

Cooperation with Saudi Arabia against Islamist terrorism is very much in the U.S. interest. Such cooperation can exist for a time largely in secret, as it does now, but it cannot grow and thrive there. Nor, on either side, can friendship be unconditional.

Recommendation: The problems in the U.S.-Saudi relationship must be confronted, openly. The United States and Saudi Arabia must determine if they can build a relationship that political leaders on both sides are prepared to publicly defend—a relationship about more than oil. It should include a shared commitment to political and economic reform, as Saudis make common cause with the outside world. It should include a shared interest in greater tolerance and cultural respect, translating into a commitment to fight the violent extremists who foment hatred.

12.3 PREVENT THE CONTINUED GROWTH OF ISLAMIST TERRORISM

In October 2003, reflecting on progress after two years of waging the global war on terrorism, Defense Secretary Donald Rumsfeld asked his advisers: "Are we capturing, killing or deterring and dissuading more terrorists every day than the madrassas and the radical clerics are recruiting, training and deploying against us? Does the US need to fashion a broad, integrated plan to stop the next generation of terrorists? The US is putting relatively little effort into a long-range plan, but we are putting a great deal of effort into trying to stop terrorists. The cost-benefit ratio is against us! Our cost is billions against the terrorists' costs of millions."[22]

These are the right questions. Our answer is that we need short-term action on a long-range strategy, one that invigorates our foreign policy with the attention that the President and Congress have given to the military and intelligence parts of the conflict against Islamist terrorism.

Engage the Struggle of Ideas

The United States is heavily engaged in the Muslim world and will be for many years to come. This American engagement is resented. Polls in 2002 found that among America's

friends, like Egypt—the recipient of more U.S. aid for the past 20 years than any other Muslim country—only 15 percent of the population had a favorable opinion of the United States. In Saudi Arabia the number was 12 percent. And two-thirds of those surveyed in 2003 in countries from Indonesia to Turkey (a NATO ally) were very or somewhat fearful that the United States may attack them.[23]

Support for the United States has plummeted. Polls taken in Islamic countries after 9/11 suggested that many or most people thought the United States was doing the right thing in its fight against terrorism; few people saw popular support for al Qaeda; half of those surveyed said that ordinary people had a favorable view of the United States. By 2003, polls showed that "the bottom has fallen out of support for America in most of the Muslim world. Negative views of the U.S. among Muslims, which had been largely limited to countries in the Middle East, have spread. . . . Since last summer, favorable ratings for the U.S. have fallen from 61% to 15% in Indonesia and from 71% to 38% among Muslims in Nigeria."[24]

Many of these views are at best uninformed about the United States and, at worst, informed by cartoonish stereotypes, the coarse expression of a fashionable "Occidentalism" among intellectuals who caricature U.S. values and policies. Local newspapers and the few influential satellite broadcasters—like al Jazeera—often reinforce the jihadist theme that portrays the United States as anti-Muslim.[25]

The small percentage of Muslims who are fully committed to Usama Bin Ladin's version of Islam are impervious to persuasion. It is among the large majority of Arabs and Muslims that we must encourage reform, freedom, democracy, and opportunity, even though our own promotion of these messages is limited in its effectiveness simply because we are its carriers. Muslims themselves will have to reflect upon such basic issues as the concept of jihad, the position of women, and the place of non-Muslim minorities. The United States can promote moderation, but cannot ensure its ascendancy. Only Muslims can do this.

The setting is diffcult. The combined gross domestic product of the 22 countries in the Arab League is less than the GDP of Spain. Forty percent of adult Arabs are illiterate, two-thirds of them women. One-third of the broader Middle East lives on less than two dollars a day. Less than 2 percent of the population has access to the Internet. The majority of older Arab youths have expressed a desire to emigrate to other countries, particularly those in Europe.[26]

In short, the United States has to help defeat an ideology, not just a group of people, and we must do so under difficult circumstances. How can the United States and its friends help moderate Muslims combat the extremist ideas?

Recommendation: The U.S. government must define what the message is, what it stands for. We should offer an example of moral leadership in the world, committed to treat people humanely, abide by the rule of law, and be generous and caring to our neighbors. America and Muslim friends can agree on respect for human dignity and opportunity. To Muslim parents, terrorists like Bin Ladin have nothing to offer their children but visions of violence and death. America and its friends have a crucial advantage—we can offer these parents a vision that might give their children a better future. If we heed the views of thoughtful leaders in the Arab and Muslim world, a moderate consensus can be found.

That vision of the future should stress life over death: individual educational and economic opportunity. This vision includes widespread political participation and contempt for

indiscriminate violence. It includes respect for the rule of law, openness in discussing differences, and tolerance for opposing points of view.

Recommendation: Where Muslim governments, even those who are friends, do not respect these principles, the United States must stand for a better future. One of the lessons of the long Cold War was that short-term gains in cooperating with the most repressive and brutal governments were too often outweighed by long-term setbacks for America's stature and interests.

American foreign policy is part of the message. America's policy choices have consequences. Right or wrong, it is simply a fact that American policy regarding the Israeli-Palestinian conflict and American actions in Iraq are dominant staples of popular commentary across the Arab and Muslim world. That does not mean U.S. choices have been wrong. It means those choices must be integrated with America's message of opportunity to the Arab and Muslim world. Neither Israel nor the new Iraq will be safer if worldwide Islamist terrorism grows stronger.

The United States must do more to communicate its message. Reflecting on Bin Ladin's success in reaching Muslim audiences, Richard Holbrooke wondered, "How can a man in a cave outcommunicate the world's leading communications society?" Deputy Secretary of State Richard Armitage worried to us that Americans have been "exporting our fears and our anger," not our vision of opportunity and hope.[27]

Recommendation: Just as we did in the Cold War, we need to defend our ideals abroad vigorously. America does stand up for its values. The United States defended, and still defends, Muslims against tyrants and criminals in Somalia, Bosnia, Kosovo, Afghanistan, and Iraq. If the United States does not act aggressively to define itself in the Islamic world, the extremists will gladly do the job for us.

- **Recognizing that Arab and Muslim audiences rely on satellite television and radio, the government has begun some promising initiatives in television and radio broadcasting to the Arab world, Iran, and Afghanistan. These efforts are beginning to reach large audiences. The Broadcasting Board of Governors has asked for much larger resources. It should get them.**
- **The United States should rebuild the scholarship, exchange, and library programs that reach out to young people and offer them knowledge and hope. Where such assistance is provided, it should be identified as coming from the citizens of the United States.**

An Agenda of Opportunity

The United States and its friends can stress educational and economic opportunity. The United Nations has rightly equated "literacy as freedom."

- The international community is moving toward setting a concrete goal—to cut the Middle East region's illiteracy rate in half by 2010, targeting women and girls and supporting programs for adult literacy.
- Unglamorous help is needed to support the basics, such as textbooks that translate more of the world's knowledge into local languages and libraries to house such materials. Education about the outside world, or other cultures, is weak.

- More vocational education is needed, too, in trades and business skills. The Middle East can also benefit from some of the programs to bridge the digital divide and increase Internet access that have already been developed for other regions of the world.

Education that teaches tolerance, the dignity and value of each individual, and respect for different beliefs is a key element in any global strategy to eliminate Islamist terrorism.

Recommendation: The U.S. government should offer to join with other nations in generously supporting a new International Youth Opportunity Fund. Funds will be spent directly for building and operating primary and secondary schools in those Muslim states that commit to sensibly investing their own money in public education.

Economic openness is essential. Terrorism is not caused by poverty. Indeed, many terrorists come from relatively well-off families. Yet when people lose hope, when societies break down, when countries fragment, the breeding grounds for terrorism are created. Backward economic policies and repressive political regimes slip into societies that are without hope, where ambition and passions have no constructive outlet.

The policies that support economic development and reform also have political implications. Economic and political liberties tend to be linked. Commerce, especially international commerce, requires ongoing cooperation and compromise, the exchange of ideas across cultures, and the peaceful resolution of differences through negotiation or the rule of law. Economic growth expands the middle class, a constituency for further reform. Successful economies rely on vibrant private sectors, which have an interest in curbing indiscriminate government power. Those who develop the practice of controlling their own economic destiny soon desire a voice in their communities and political societies.

The U.S. government has announced the goal of working toward a Middle East Free Trade Area, or MEFTA, by 2013. The United States has been seeking comprehensive free trade agreements (FTAs) with the Middle Eastern nations most firmly on the path to reform. The U.S.-Israeli FTA was enacted in 1985, and Congress implemented an FTA with Jordan in 2001. Both agreements have expanded trade and investment, thereby supporting domestic economic reform. In 2004, new FTAs were signed with Morocco and Bahrain, and are awaiting congressional approval. These models are drawing the interest of their neighbors. Muslim countries can become full participants in the rules-based global trading system, as the United States considers lowering its trade barriers with the poorest Arab nations.

Recommendation: A comprehensive U.S. Strategy to counter terrorism should include economic policies that encourage development, more open societies, and opportunities for people to improve the lives of their families and to enhance prospects for their children's future.

Turning a National Strategy into a Coalition Strategy

Practically every aspect of U.S. counterterrorism strategy relies on international cooperation. Since 9/11, these contacts concerning military, law enforcement, intelligence, travel and customs, and financial matters have expanded so dramatically, and often in an ad hoc way, that it is difficult to track these efforts, much less integrate them.

Recommendation: The United States should engage other nations in developing a comprehensive coalition strategy against Islamist terrorism. There are several multilateral institutions in which such issues should be addressed. But the most important policies should be discussed and coordinated in a flexible contact group of leading coalition governments. This is a good place, for example, to develop joint strategies for targeting terrorist travel, or for hammering out a common strategy for the places where terrorists may be finding sanctuary.

Presently the Muslim and Arab states meet with each other, in organizations such as the Islamic Conference and the Arab League. The Western states meet with each other in organizations such as NATO and the Group of Eight summit of leading industrial nations. A recent G-8 summit initiative to begin a dialogue about reform may be a start toward finding a place where leading Muslim states can discuss—and be seen to discuss—critical policy issues with the leading Western powers committed to the future of the Arab and Muslim world.

These new international efforts can create durable habits of visible cooperation, as states willing to step up to their responsibilities join together in constructive efforts to direct assistance and coordinate action.

Coalition warfare also requires coalition policies on what to do with enemy captives. Allegations that the United States abused prisoners in its custody make it harder to build the diplomatic, political, and military alliances the government will need. The United States should work with friends to develop mutually agreed-on principles for the detention and humane treatment of captured international terrorists who are not being held under a particular country's criminal laws. Countries such as Britain, Australia, and Muslim friends, are committed to fighting terrorists. America should be able to reconcile its views on how to balance humanity and security with our nation's commitment to these same goals.

The United States and some of its allies do not accept the application of full Geneva Convention treatment of prisoners of war to captured terrorists. Those Conventions establish a minimum set of standards for prisoners in internal conflicts. Since the international struggle against Islamist terrorism is not internal, those provisions do not formally apply, but they are commonly accepted as basic standards for humane treatment.

Recommendation: The United States should engage its friends to develop a common coalition approach toward the detention and humane treatment of captured terrorists. New principles might draw upon Article 3 of the Geneva Conventions on the law of armed conflict. That article was specifically designed for those cases in which the usual laws of war did not apply. Its minimum standards are generally accepted throughout the world as customary international law.

Proliferation of Weapons of Mass Destruction

The greatest danger of another catastrophic attack in the United States will materialize if the world's most dangerous terrorists acquire the world's most dangerous weapons. As we note in chapter 2, al Qaeda has tried to acquire or make nuclear weapons for at least ten years. In chapter 4, we mentioned officials worriedly discussing, in 1998, reports that Bin Ladin's associates thought their leader was intent on carrying out a "Hiroshima."

These ambitions continue. In the public portion of his February 2004 worldwide threat assessment to Congress, DCI Tenet noted that Bin Ladin considered the acquisition of

weapons of mass destruction to be a "religious obligation." He warned that al Qaeda "continues to pursue its strategic goal of obtaining a nuclear capability." Tenet added that "more than two dozen other terrorist groups are pursuing CBRN [chemical, biological, radiological, and nuclear] materials."[28]

A nuclear bomb can be built with a relatively small amount of nuclear material. A trained nuclear engineer with an amount of highly enriched uranium or plutonium about the size of a grapefruit or an orange, together with commercially available material, could fashion a nuclear device that would fit in a van like the one RamziYousef parked in the garage of the World Trade Center in 1993. Such a bomb would level Lower Manhattan.[29]

The coalition strategies we have discussed to combat Islamist terrorism should therefore be combined with a parallel, vital effort to prevent and counter the proliferation of weapons of mass destruction (WMD).We recommend several initiatives in this area.

STRENGTHEN COUNTERPROLIFERATION EFFORTS.

While efforts to shut down Libya's illegal nuclear program have been generally successful, Pakistan's illicit trade and the nuclear smuggling networks of Pakistani scientist A.Q. Khan have revealed that the spread of nuclear weapons is a problem of global dimensions. Attempts to deal with Iran's nuclear program are still underway. Therefore, the United States should work with the international community to develop laws and an international legal regime with universal jurisdiction to enable the capture, interdiction, and prosecution of such smugglers by any state in the world where they do not disclose their activities.

EXPAND THE PROLIFERATION SECURITY INITIATIVE.

In May 2003, the Bush administration announced the Proliferation Security Initiative (PSI): nations in a willing partnership combining their national capabilities to use military, economic, and diplomatic tools to interdict threatening shipments of WMD and missile-related technology.

The PSI can be more effective if it uses intelligence and planning resources of the NATO alliance. Moreover, PSI membership should be open to non-NATO countries. Russia and China should be encouraged to participate.

SUPPORT THE COOPERATIVE THREAT REDUCTION PROGRAM.

Outside experts are deeply worried about the U.S. government's commitment and approach to securing the weapons and highly dangerous materials still scattered in Russia and other countries of the Soviet Union. The government's main instrument in this area, the Cooperative Threat Reduction Program (usually referred to as "Nunn-Lugar," after the senators who sponsored the legislation in 1991), is now in need of expansion, improvement, and resources. The U.S. government has recently redoubled its international commitments to support this program, and we recommend that the United States do all it can, if Russia and other countries will do their part. The government should weigh the value of this investment against the catastrophic cost America would face should such weapons find their way to the terrorists who are so anxious to acquire them.

Recommendation: Our report shows that al Qaeda has tried to acquire or make weapons of mass destruction for at least ten years. There is no doubt the United States

would be a prime target. Preventing the proliferation of these weapons warrants a maximum effort—by strengthening counterproliferation efforts, expanding the Proliferation Security Initiative, and supporting the Cooperative Threat Reduction program.

Targeting Terrorist Money

The general public sees attacks on terrorist finance as a way to "starve the terrorists of money." So, initially, did the U.S. government. After 9/11, the United States took aggressive actions to designate terrorist financiers and freeze their money, in the United States and through resolutions of the United Nations. These actions appeared to have little effect and, when confronted by legal challenges, the United States and the United Nations were often forced to unfreeze assets.

The difficulty, understood later, was that even if the intelligence community might "link" someone to a terrorist group through acquaintances or communications, the task of tracing the money from that individual to the terrorist group, or otherwise showing complicity, was far more difficult. It was harder still to do so without disclosing secrets.

These early missteps made other countries unwilling to freeze assets or otherwise act merely on the basis of a U.S. action. Multilateral freezing mechanisms now require waiting periods before being put into effect, eliminating the element of surprise and thus virtually ensuring that little money is actually frozen. Worldwide asset freezes have not been adequately enforced and have been easily circumvented, often within weeks, by simple methods.

But trying to starve the terrorists of money is like trying to catch one kind of fish by draining the ocean. A better strategy has evolved since those early months, as the government learned more about how al Qaeda raises, moves, and spends money.

Recommendation: Vigorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts. The government has recognized that information about terrorist money helps us to understand their networks, search them out, and disrupt their operations. Intelligence and law enforcement have targeted the relatively small number of financial facilitators—individuals al Qaeda relied on for their ability to raise and deliver money—at the core of al Qaeda's revenue stream. These efforts have worked. The death or capture of several important facilitators has decreased the amount of money available to al Qaeda and has increased its costs and difficulty in raising and moving that money. Captures have additionally provided a windfall of intelligence that can be used to continue the cycle of disruption.

The U.S. financial community and some international financial institutions have generally provided law enforcement and intelligence agencies with extraordinary cooperation, particularly in supplying information to support quickly developing investigations. Obvious vulnerabilities in the U.S. financial system have been corrected. The United States has been less successful in persuading other countries to adopt financial regulations that would permit the tracing of financial transactions.

Public designation of terrorist financiers and organizations is still part of the fight, but it is not the primary weapon. Designations are instead a form of diplomacy, as governments join together to identify named individuals and groups as terrorists. They also prevent open

fundraising. Some charities that have been identified as likely avenues for terrorist financing have seen their donations diminish and their activities come under more scrutiny, and others have been put out of business, although controlling overseas branches of Gulf-area charities remains a challenge. The Saudi crackdown after the May 2003 terrorist attacks in Riyadh has apparently reduced the funds available to al Qaeda—perhaps drastically—but it is too soon to know if this reduction will last.

Though progress apparently has been made, terrorists have shown considerable creativity in their methods of moving money. If al Qaeda is replaced by smaller, decentralized terrorist groups, the premise behind the government's efforts—that terrorists need a financial support network—may become outdated. Moreover, some terrorist operations do not rely on outside sources of money and may now be self-funding, either through legitimate employment or low-level criminal activity.[30]

12.4 PROTECT AGAINST AND PREPARE FOR TERRORIST ATTACKS

In the nearly three years since 9/11, Americans have become better protected against terrorist attack. Some of the changes are due to government action, such as new precautions to protect aircraft. A portion can be attributed to the sheer scale of spending and effort. Publicity and the vigilance of ordinary Americans also make a difference.

But the President and other officials acknowledge that although Americans may be safer, they are not safe. Our report shows that the terrorists analyze defenses. They plan accordingly. Defenses cannot achieve perfect safety. They make targets harder to attack successfully, and they deter attacks by making capture more likely. Just increasing the attacker's odds of failure may make the difference between a plan attempted, or a plan discarded. The enemy also may have to develop more elaborate plans, thereby increasing the danger of exposure or defeat.

Protective measures also prepare for the attacks that may get through, containing the damage and saving lives.

Terrorist Travel

More than 500 million people annually cross U.S. borders at legal entry points, about 330 million of them noncitizens. Another 500,000 or more enter illegally without inspection across America's thousands of miles of land borders or remain in the country past the expiration of their permitted stay. The challenge for national security in an age of terrorism is to prevent the very few people who may pose overwhelming risks from entering or remaining in the United States undetected.[31]

In the decade before September 11, 2001, border security—encompassing travel, entry, and immigration—was not seen as a national security matter. Public figures voiced concern about the "war on drugs," the right level and kind of immigration, problems along the southwest border, migration crises originating in the Caribbean and elsewhere, or the growing criminal traffic in humans. The immigration system as a whole was widely viewed as increasingly dysfunctional and badly in need of reform. In national security circles, however, only smuggling of weapons of mass destruction carried weight, not the entry of terrorists who might use such weapons or the presence of associated foreign-born terrorists.

For terrorists, travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. To them, international travel presents great danger, because they must surface to pass through regulated channels, present themselves to border security officials, or attempt to circumvent inspection points.

In their travels, terrorists use evasive methods, such as altered and counterfeit passports and visas, specific travel methods and routes, liaisons with corrupt government officials, human smuggling networks, supportive travel agencies, and immigration and identity fraud. These can sometimes be detected.

Before 9/11, no agency of the U.S. government systematically analyzed terrorists' travel strategies. Had they done so, they could have discovered the ways in which the terrorist predecessors to al Qaeda had been systematically but detectably exploiting weaknesses in our border security since the early 1990s.

We found that as many as 15 of the 19 hijackers were potentially vulnerable to interception by border authorities. Analyzing their characteristic travel documents and travel patterns could have allowed authorities to intercept 4 to 15 hijackers and more effective use of information available in U.S. government databases could have identified up to 3 hijackers.[32]

Looking back, we can also see that the routine operations of our immigration laws—that is, aspects of those laws not specifically aimed at protecting against terrorism—inevitably shaped al Qaeda's planning and opportunities. Because they were deemed not to be bona fide tourists or students as they claimed, five conspirators that we know of tried to get visas and failed, and one was denied entry by an inspector. We also found that had the immigration system set a higher bar for determining whether individuals are who or what they claim to be—and ensuring routine consequences for violations—it could potentially have excluded, removed, or come into further contact with several hijackers who did not appear to meet the terms for admitting short-term visitors.[33]

Our investigation showed that two systemic weaknesses came together in our border system's inability to contribute to an effective defense against the 9/11 attacks: a lack of well-developed counterterrorism measures as a part of border security and an immigration system not able to deliver on its basic commitments, much less support counterterrorism. These weaknesses have been reduced but are far from being overcome.

Recommendation: Targeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility.

Since 9/11, significant improvements have been made to create an integrated watchlist that makes terrorist name information available to border and law enforcement authorities. However, in the already difficult process of merging border agencies in the new Department of Homeland Security—"changing the engine while flying" as one official put it[34]—new insights into terrorist travel have not yet been integrated into the front lines of border security.

The small terrorist travel intelligence collection and analysis program currently in place has produced disproportionately useful results. It should be expanded. Since officials at the borders encounter travelers and their documents first and investigate travel facilitators, they must work closely with intelligence officials.

Internationally and in the United States, constraining terrorist travel should become a vital part of counterterrorism strategy. Better technology and training to detect terrorist travel documents are the most important immediate steps to reduce America's vulnerability to clandestine entry. Every stage of our border and immigration system should have as a part of its operations the detection of terrorist indicators on travel documents. Information systems able to authenticate travel documents and detect potential terrorist indicators should be used at consulates, at primary border inspection lines, in immigration services offices, and in intelligence and enforcement units. All frontline personnel should receive some training. Dedicated specialists and ongoing linkages with the intelligence community are also required. The Homeland Security Department's Directorate of Information Analysis and Infrastructure Protection should receive more resources to accomplish its mission as the bridge between the frontline border agencies and the rest of the government counterterrorism community.

A Biometric Screening System

When people travel internationally, they usually move through defined channels, or portals. They may seek to acquire a passport. They may apply for a visa. They stop at ticket counters, gates, and exit controls at airports and seaports. Upon arrival, they pass through inspection points. They may transit to another gate to get on an airplane. Once inside the country, they may seek another form of identification and try to enter a government or private facility. They may seek to change immigration status in order to remain.

Each of these checkpoints or portals is a screening—a chance to establish that people are who they say they are and are seeking access for their stated purpose, to intercept identifiable suspects, and to take effective action.

The job of protection is shared among these many defined checkpoints. By taking advantage of them all, we need not depend on any one point in the system to do the whole job. The challenge is to see the common problem across agencies and functions and develop a conceptual framework—an architecture—for an effective screening system.[35]

Throughout government, and indeed in private enterprise, agencies and firms at these portals confront recurring judgments that balance security, efficiency, and civil liberties. These problems should be addressed systemically, not in an ad hoc, fragmented way. For example:

what information is an individual required to present and in what form?

A fundamental problem, now beginning to be addressed, is the lack of standardized information in "feeder" documents used in identifying individuals. Biometric identifiers that measure unique physical characteristics, such as facial features, fingerprints, or iris scans, and reduce them to digitized, numerical statements called algorithms, are just beginning to be used. Travel history, however, is still recorded in passports with entry-exit stamps called cachets, which al Qaeda has trained its operatives to forge and use to conceal their terrorist activities.

how will the individual and the information be checked?

There are many databases just in the United States—for terrorist, criminal, and immigration history, as well as financial information, for instance. Each is set up for different purposes

and stores different kinds of data, under varying rules of access. Nor is access always guaranteed. Acquiring information held by foreign governments may require painstaking negotiations, and records that are not yet digitized are difficult to search or analyze. The development of terrorist indicators has hardly begun, and behavioral cues remain important.

WHO WILL SCREEN INDIVIDUALS, AND WHAT WILL THEY BE TRAINED TO DO?

A wide range of border, immigration, and law enforcement officials encounter visitors and immigrants and they are given little training in terrorist travel intelligence. Fraudulent travel documents, for instance, are usually returned to travelers who are denied entry without further examination for terrorist trademarks, investigation as to their source, or legal process.

WHAT ARE THE CONSEQUENCES OF FINDING A SUSPICIOUS INDICATOR, AND WHO WILL TAKE ACTION?

One risk is that responses may be ineffective or produce no further information. Four of the 9/11 attackers were pulled into secondary border inspection, but then admitted. More than half of the 19 hijackers were flagged by the Federal Aviation Administration's profiling system when they arrived for their flights, but the consequence was that bags, not people, were checked. Competing risks include "false positives," or the danger that rules may be applied with insufficient training or judgment. Overreactions can impose high costs too—on individuals, our economy, and our beliefs about justice.

- A special note on the importance of trusting subjective judgment: One potential hijacker was turned back by an immigration inspector as he tried to enter the United States. The inspector relied on intuitive experience to ask questions more than he relied on any objective factor that could be detected by "scores" or a machine. Good people who have worked in such jobs for a long time understand this phenomenon well. Other evidence we obtained confirmed the importance of letting experienced gate agents or security screeners ask questions and use their judgment. This is not an invitation to arbitrary exclusions. But any effective system has to grant some scope, perhaps in a little extra inspection or one more check, to the instincts and discretion of well trained human beings.

Recommendation: The U.S. border security system should be integrated into a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with systemwide goals in mind. Extending those standards among other governments could dramatically strengthen America and the world's collective ability to intercept individuals who pose catastrophic threats.

We advocate a system for screening, not categorical profiling. A screening system looks for particular, identifiable suspects or indicators of risk. It does not involve guesswork about who might be dangerous. It requires frontline border officials who have the tools and

resources to establish that people are who they say they are, intercept identifiable suspects, and disrupt terrorist operations.

The U.S. Border Screening System

The border and immigration system of the United States must remain a visible manifestation of our belief in freedom, democracy, global economic growth, and the rule of law, yet serve equally well as a vital element of counterterrorism. Integrating terrorist travel information in the ways we have described is the most immediate need. But the underlying system must also be sound.

Since September 11, the United States has built the first phase of a biometric screening program, called US VISIT (the United States Visitor and Immigrant Status Indicator Technology program). It takes two bioretric identifiers—digital photographs and prints of two index fingers—from travelers. False identities are used by terrorists to avoid being detected on a watchlist. These biometric identifiers make such evasions far more difficult.

So far, however, only visitors who acquire visas to travel to the United States are covered. While visitors from "visa waiver" countries will be added to the program, beginning this year, covered travelers will still constitute only about 12 percent of all noncitizens crossing U.S. borders. Moreover, exit data are not uniformly collected and entry data are not fully automated. It is not clear the system can be installed before 2010, but even this timetable may be too slow, given the possible security dangers.[36]

- Americans should not be exempt from carrying biometric passports or otherwise enabling their identities to be securely verified when they enter the United States; nor should Canadians or Mexicans. Currently U.S. persons are exempt from carrying passports when returning from Canada, Mexico, and the Caribbean. The current system enables non-U.S. citizens to gain entry by showing minimal identification. The 9/11 experience shows that terrorists study and exploit America's vulnerabilities.
- To balance this measure, programs to speed known travelers should be a higher priority, permitting inspectors to focus on greater risks. The daily commuter should not be subject to the same measures as first-time travelers. An individual should be able to preenroll, with his or her identity verified in passage. Updates of database information and other checks can ensure ongoing reliability. The solution, requiring more research and development, is likely to combine radio frequency technology with biometric identifiers.[37]
- The current patchwork of border screening systems, including several frequent traveler programs, should be consolidated with the US VISIT system to enable the development of an integrated system, which in turn can become part of the wider screening plan we suggest.
- The program allowing individuals to travel from foreign countries through the United States to a third country, without having to obtain a U.S. visa, has been suspended. Because "transit without visa" can be exploited by terrorists to enter the United States, the program should not be reinstated unless and until transit passage areas can be fully secured to prevent passengers from illegally exiting the airport.

Inspectors adjudicating entries of the 9/11 hijackers lacked adequate information and knowledge of the rules. All points in the border system—from consular offices to immigration services offices—will need appropriate electronic access to an individual's file. Scattered units at Homeland Security and the State Department perform screening and data mining: instead, a government-wide team of border and transportation officials should be working together. A modern border and immigration system should combine a biometric entry-exit system with accessible files on visitors and immigrants, along with intelligence on indicators of terrorist travel.

Our border screening system should check people efficiently and welcome friends. Admitting large numbers of students, scholars, businesspeople, and tourists fuels our economy, cultural vitality, and political reach. There is evidence that the present system is disrupting travel to the United States. Overall, visa applications in 2003 were down over 32 percent since 2001. In the Middle East, they declined about 46 percent. Training and the design of security measures should be continuously adjusted.[38]

Recommendation: The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system, including a single system for speeding qualified travelers. It should be integrated with the system that provides benefits to foreigners seeking to stay in the United States. Linking biometric passports to good data systems and decisionmaking is a fundamental goal. No one can hide his or her debt by acquiring a credit card with a slightly different name. Yet today, a terrorist can defeat the link to electronic records by tossing away an old passport and slightly altering the name in the new one.

Completion of the entry-exit system is a major and expensive challenge. Biometrics have been introduced into an antiquated computer environment. Replacement of these systems and improved biometric systems will be required. Nonetheless, funding and completing a biometrics-based entry-exit system is an essential investment in our national security.

Exchanging terrorist information with other countries, consistent with privacy requirements, along with listings of lost and stolen passports, will have immediate security benefits. We should move toward real-time verification of passports with issuing authorities. The further away from our borders that screening occurs, the more security benefits we gain. At least some screening should occur before a passenger departs on a flight destined for the United States. We should also work with other countries to ensure effective inspection regimes at all airports.[39]

The international community arrives at international standards for the design of passports through the International Civil Aviation Organization (ICAO). The global standard for identification is a digital photograph; fingerprints are optional.We must work with others to improve passport standards and provide foreign assistance to countries that need help in making the transition.[40]

Recommendation: The U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation.

Immigration Law and Enforcement

Our borders and immigration system, including law enforcement, ought to send a message of welcome, tolerance, and justice to members of immigrant communities in the United States and in their countries of origin. We should reach out to immigrant communities. Good immigration services are one way of doing so that is valuable in every way—including intelligence.

It is elemental to border security to know who is coming into the country. Today more than 9 million people are in the United States outside the legal immigration system. We must also be able to monitor and respond to entrances between our ports of entry, working with Canada and Mexico as much as possible.

There is a growing role for state and local law enforcement agencies. They need more training and work with federal agencies so that they can cooperate more effectively with those federal authorities in identifying terrorist suspects.

All but one of the 9/11 hijackers acquired some form of U.S. identification document, some by fraud. Acquisition of these forms of identification would have assisted them in boarding commercial flights, renting cars, and other necessary activities.

Recommendation: Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.[41]

Strategies for Aviation and Transportation Security

The U.S. transportation system is vast and, in an open society, impossible to secure completely against terrorist attacks. There are hundreds of commercial airports, thousands of planes, and tens of thousands of daily flights carrying more than half a billion passengers a year. Millions of containers are imported annually through more than 300 sea and river ports served by more than 3,700 cargo and passenger terminals. About 6,000 agencies provide transit services through buses, subways, ferries, and light-rail service to about 14 million Americans each weekday.[42]

In November 2001, Congress passed and the President signed the Aviation and Transportation Security Act. This act created the Transportation Security Administration (TSA), which is now part of the Homeland Security Department. In November 2002, both the Homeland Security Act and the Maritime Transportation Security Act followed. These laws required the development of strategic plans to describe how the new department and TSA would provide security for critical parts of the U.S. transportation sector.

Over 90 percent of the nation's $5.3 billion annual investment in the TSA goes to aviation—to fight the last war. The money has been spent mainly to meet congressional mandates to federalize the security checkpoint screeners and to deploy existing security methods and technologies at airports. The current efforts do not yet reflect a forward-looking strategic plan systematically analyzing assets, risks, costs, and benefits. Lacking such a plan, we are not convinced that our transportation security resources are being allocated to the greatest risks in a cost-effective way.

- Major vulnerabilities still exist in cargo and general aviation security. These, together with inadequate screening and access controls, continue to present aviation security challenges.
- While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime or surface transportation. Initiatives to secure shipping containers have just begun. Surface transportation systems such as railroads and mass transit remain hard to protect because they are so accessible and extensive.

Despite congressional deadlines, the TSA has developed neither an integrated strategic plan for the transportation sector nor specific plans for the various modes—air, sea, and ground.

Recommendation: Hard choices must be made in allocating limited resources. The U.S. government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort. The plan should assign roles and missions to the relevant authorities (federal, state, regional, and local) and to private stakeholders. In measuring effectiveness, perfection is unattainable. But terrorists should perceive that potential targets are defended. They may be deterred by a significant chance of failure.

Congress should set a specific date for the completion of these plans and hold the Department of Homeland Security and TSA accountable for achieving them.

The most powerful investments may be for improvements in technologies with applications across the transportation modes, such as scanning technologies designed to screen containers that can be transported by plane, ship, truck, or rail. Though such technologies are becoming available now, widespread deployment is still years away.

In the meantime, the best protective measures may be to combine improved methods of identifying and tracking the high-risk containers, operators, and facilities that require added scrutiny with further efforts to integrate intelligence analysis, effective procedures for transmitting threat information to transportation authorities, and vigilance by transportation authorities and the public.

A Layered Security System

No single security measure is foolproof. Accordingly, the TSA must have multiple layers of security in place to defeat the more plausible and dangerous forms of attack against public transportation.

- The plan must take into consideration the full array of possible enemy tactics, such as use of insiders, suicide terrorism, or standoff attack. Each layer must be effective in its own right. Each must be supported by other layers that are redundant and coordinated.
- The TSA should be able to identify for Congress the array of potential terrorist attacks, the layers of security in place, and the reliability provided by each layer. TSA must develop a plan as described above to improve weak individual layers and the effectiveness of the layered systems it deploys.

On 9/11, the 19 hijackers were screened by a computer-assisted screening system called CAPPS. More than half were identified for further inspection, which applied only to their checked luggage.

Under current practices, air carriers enforce government orders to stop certain known and suspected terrorists from boarding commercial flights and to apply secondary screening procedures to others. The "no-fly" and "automatic selectee" lists include only those individuals who the U.S. government believes pose a direct threat of attacking aviation.

Because air carriers implement the program, concerns about sharing intelligence information with private firms and foreign countries keep the U.S. government from listing all terrorist and terrorist suspects who should be included. The TSA has planned to take over this function when it deploys a new screening system to take the place of CAPPS. The deployment of this system has been delayed because of claims it may violate civil liberties.

Recommendation: Improved use of "no-fly" and "automatic selectee" lists should not be delayed while the argument about a successor to CAPPS continues. This screening function should be performed by the TSA, and it should utilize the larger set of watchlists maintained by the federal government. Air carriers should be required to supply the information needed to test and implement this new system.

CAPPS is still part of the screening process, still profiling passengers, with the consequences of selection now including personal searches of the individual and carry-on bags. The TSA is dealing with the kind of screening issues that are being encountered by other agencies. As we mentioned earlier, these screening issues need to be elevated for high-level attention and addressed promptly by the government. Working through these problems can help clear the way for the TSA's screening improvements and would help many other agencies too.

The next layer is the screening checkpoint itself. As the screening system tries to stop dangerous people, the checkpoint needs to be able to find dangerous items. Two reforms are needed soon: (1) screening people for explosives, not just their carry-on bags, and (2) improving screener performance.

Recommendation: The TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. As a start, each individual selected for special screening should be screened for explosives. Further, the TSA should conduct a human factors study, a method often used in the private sector, to understand problems in screener performance and set attainable objectives for individual screeners and for the checkpoints where screening takes place.

Concerns also remain regarding the screening and transport of checked bags and cargo. More attention and resources should be directed to reducing or mitigating the threat posed by explosives in vessels' cargo holds. The TSA should expedite the installation of advanced (in-line) baggage-screening equipment. Because the aviation industry will derive substantial benefits from this deployment, it should pay a fair share of the costs. The TSA should require that every passenger aircraft carrying cargo must deploy at least one hardened container to carry any suspect cargo. TSA also needs to intensify its efforts to identify, track, and appropriately screen potentially dangerous cargo in both the aviation and maritime sectors.

The Protection of Civil Liberties

Many of our recommendations call for the government to increase its presence in our lives—for example, by creating standards for the issuance of forms of identification, by better securing our borders, by sharing information gathered by many different agencies. We also recommend the consolidation of authority over the now far-flung entities constituting the intelligence community. The Patriot Act vests substantial powers in our federal government. We have seen the government use the immigration laws as a tool in its counterterrorism effort. Even without the changes we recommend, the American public has vested enormous authority in the U.S. government.

At our first public hearing on March 31, 2003, we noted the need for balance as our government responds to the real and ongoing threat of terrorist attacks. The terrorists have used our open society against us. In wartime, government calls for greater powers, and then the need for those powers recedes after the war ends. This struggle will go on. Therefore, while protecting our homeland, Americans should be mindful of threats to vital personal and civil liberties. This balancing is no easy task, but we must constantly strive to keep it right.

This shift of power and authority to the government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life. We therefore make three recommendations.

First, as we will discuss in chapter 13, to open up the sharing of information across so many agencies and with the private sector, the President should take responsibility for determining what information can be shared by which agencies and under what conditions. Protection of privacy rights should be one key element of this determination.

Recommendation: As the President determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared.

Second, Congress responded, in the immediate aftermath of 9/11, with the Patriot Act, which vested substantial new powers in the investigative agencies of the government. Some of the most controversial provisions of the Patriot Act are to "sunset" at the end of 2005. Many of the act's provisions are relatively noncontroversial, updating America's surveillance laws to reflect technological developments in a digital age. Some executive actions that have been criticized are unrelated to the Patriot Act. The provisions in the act that facilitate the sharing of information among intelligence agencies and between law enforcement and intelligence appear, on balance, to be beneficial. Because of concerns regarding the shifting balance of power to the government, we think that a full and informed debate on the Patriot Act would be healthy.

Recommendation: The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use.

Third, during the course of our inquiry, we were told that there is no office within the government whose job it is to look across the government at the actions we are taking to protect ourselves to ensure that liberty concerns are appropriately considered. If, as we

recommend, there is substantial change in the way we collect and share intelligence, there should be a voice within the executive branch for those concerns. Many agencies have privacy offices, albeit of limited scope. The Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board has, in the past, had the job of overseeing certain activities of the intelligence community.

Recommendation: At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties.

We must find ways of reconciling security with liberty, since the success of one helps protect the other. The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend.

Setting Priorities for National Preparedness

Before 9/11, no executive department had, as its first priority, the job of defending America from domestic attack. That changed with the 2002 creation of the Department of Homeland Security. This department now has the lead responsibility for problems that feature so prominently in the 9/11 story, such as protecting borders, securing transportation and other parts of our critical infrastructure, organizing emergency assistance, and working with the private sector to assess vulnerabilities.

Throughout the government, nothing has been harder for officials—executive or legislative—than to set priorities, making hard choices in allocating limited resources. These difficulties have certainly afflicted the Department of Homeland Security, hamstrung by its many congressional overseers. In delivering assistance to state and local governments, we heard—especially in New York—about imbalances in the allocation of money. The argument concentrates on two questions.

First, how much money should be set aside for criteria not directly related to risk? Currently a major portion of the billions of dollars appropriated for state and local assistance is allocated so that each state gets a certain amount, or an allocation based on its population—wherever they live.

Recommendation: Homeland security assistance should be based strictly on an assessment of risks and vulnerabilities. Now, in 2004, Washington, D.C., and New York City are certainly at the top of any such list. We understand the contention that every state and city needs to have some minimum infrastructure for emergency response. But federal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks or vulnerabilities that merit additional support. Congress should not use this money as a pork barrel.

The second question is, Can useful criteria to measure risk and vulnerability be developed that assess all the many variables? The allocation of funds should be based on an assessment of threats and vulnerabilities. That assessment should consider such factors

as population, population density, vulnerability, and the presence of critical infrastructure within each state. In addition, the federal government should require each state receiving federal emergency preparedness funds to provide an analysis based on the same criteria to justify the distribution of funds in that state.

In a free-for-all over money, it is understandable that representatives will work to protect the interests of their home states or districts. But this issue is too important for politics as usual to prevail. Resources must be allocated according to vulnerabilities. We recommend that a panel of security experts be convened to develop written benchmarks for evaluating community needs. We further recommend that federal homeland security funds be allocated in accordance with those benchmarks, and that states be required to abide by those benchmarks in disbursing the federal funds. The benchmarks will be imperfect and subjective; they will continually evolve. But hard choices must be made. Those who would allocate money on a different basis should then defend their view of the national interest.

Command, Control, and Communications

The attacks on 9/11 demonstrated that even the most robust emergency response capabilities can be overwhelmed if an attack is large enough. Teamwork, collaboration, and cooperation at an incident site are critical to a successful response. Key decisionmakers who are represented at the incident command level help to ensure an effective response, the efficient use of resources, and responder safety. Regular joint training at all levels is, moreover, essential to ensuring close coordination during an actual incident.

Recommendation: Emergency response agencies nationwide should adopt the Incident Command System (ICS). When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command. Both are proven frameworks for emergency response. We strongly support the decision that federal homeland security funding will be contingent, as of October 1, 2004, upon the adoption and regular use of ICS and unified command procedures. In the future, the Department of Homeland Security should consider making funding contingent on aggressive and realistic training in accordance with ICS and unified command procedures.

The attacks of September 11, 2001 overwhelmed the response capacity of most of the local jurisdictions where the hijacked airliners crashed. While many jurisdictions have established mutual aid compacts, a serious obstacle to multi-jurisdictional response has been the lack of indemnification for mutual-aid responders in areas such as the National Capital Region.

Public safety organizations, chief administrative officers, state emergency management agencies, and the Department of Homeland Security should develop a regional focus within the emergency responder community and promote multi-jurisdictional mutual assistance compacts. Where such compacts already exist, training in accordance with their terms should be required. Congress should pass legislation to remedy the long-standing indemnification and liability impediments to the provision of public safety mutual aid in the National Capital Region and where applicable throughout the nation.

The inability to communicate was a critical element at the World Trade Center, Pentagon, and Somerset County, Pennsylvania, crash sites, where multiple agencies and multiple jurisdictions responded. The occurrence of this problem at three very different

sites is strong evidence that compatible and adequate communications among public safety organizations at the local, state, and federal levels remains an important problem.

Recommendation: Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes. Furthermore, high-risk urban areas such as New York City and Washington, D.C., should establish signal corps units to ensure communications connectivity between and among civilian authorities, local first responders, and the National Guard. Federal funding of such units should be given high priority by Congress.

Private-Sector Preparedness

The mandate of the Department of Homeland Security does not end with government; the department is also responsible for working with the private sector to ensure preparedness. This is entirely appropriate, for the private sector controls 85 percent of the critical infrastructure in the nation. Indeed, unless a terrorist's target is a military or other secure government facility, the "first" first responders will almost certainly be civilians. Homeland security and national preparedness therefore often begins with the private sector.

Preparedness in the private sector and public sector for rescue, restart, and recovery of operations should include (1) a plan for evacuation, (2) adequate communications capabilities, and (3) a plan for continuity of operations. As we examined the emergency response to 9/11, witness after witness told us that despite 9/11, the private sector remains largely unprepared for a terrorist attack. We were also advised that the lack of a widely embraced private-sector preparedness standard was a principal contributing factor to this lack of preparedness.

We responded by asking the American National Standards Institute (ANSI) to develop a consensus on a "National Standard for Preparedness" for the private sector. ANSI convened safety, security, and business continuity experts from a wide range of industries and associations, as well as from federal, state, and local government stakeholders, to consider the need for standards for private sector emergency preparedness and business continuity.

The result of these sessions was ANSI's recommendation that the Commission endorse a voluntary National Preparedness Standard. Based on the existing American National Standard on Disaster/Emergency Management and Business Continuity Programs (NFPA 1600), the proposed National Preparedness Standard establishes a common set of criteria and terminology for preparedness, disaster management, emergency management, and business continuity programs. The experience of the private sector in the World Trade Center emergency demonstrated the need for these standards.

Recommendation: We endorse the American National Standards Institute's recommended standard for private preparedness. We were encouraged by Secretary Tom Ridge's praise of the standard, and urge the Department of Homeland Security to promote its adoption. We also encourage the insurance and credit-rating industries to look closely at a company's compliance with the ANSI standard in assessing its insurability and creditworthiness. We believe that compliance with the standard should define the standard of care owed by a company to its employees and the public for legal purposes. Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security.

NOTES

1. For spending totals, see David Baumann, "Accounting for the Deficit," *National Journal*, June 12, 2004, p. 1852 (combining categories for defense discretionary, homeland security, and international affairs).

2. White House press release, "National Strategy for Combating Terrorism," Feb. 2003 (online at www.whitehouse.gov/news/releases/2003/02/20030214-7.html).

3. "Islamist terrorism is an immediate derivative of *Islamism*. This term distinguishes itself from *Islamic* by the fact that the latter refers to a religion and culture in existence over a millennium, whereas the first is a political/religious phenomenon linked to the great events of the 20th century. Furthermore Islamists define themselves as 'Islamiyyoun/Islamists' precisely to differentiate themselves from 'Muslimun/Muslims.' . . . Islamism is defined as 'an Islamic millitant, anti-democratic movement, bearing a holistic vision of Islam whose final aim is the restoration of the caliphate.' " Mehdi Mozaffari, "Bin Laden and Islamist Terrorism," *Militaert Tidsskrift*, vol. 131 (Mar. 2002), p. 1 (online at www.mirkflem.pup.blueyonder.co.uk/pdf/islamistterrorism.pdf). The Islamist movement, born about 1940, is a product of the modern world, influenced by Marxist-Leninist concepts about revolutionary organization. "Islamists consider Islam to be as much a religion as an 'ideology,' a neologism which they introduced and which remains anathema to the ulamas (the clerical scholars)." Olivier Roy, *The Failure of Political Islam*, trans. Carol Volk (Harvard Univ. Press, 1994), p. 3. Facing political limits by the end of the 1990s, the extremist wing of the Islamist movement "rejected the democratic references invoked by the moderates; and as a result, raw terrorism in its most spectacular and destructive form became its main option for reviving armed struggle in the new millennium." Gilles Kepel, *Jihad: The Trail of Political Islam*, trans. Anthony Roberts (Harvard Univ. Press, 2002), p. 14.

4. Opening the Islamic Conference of Muslim leaders from around the world on October 16, 2003, then Malaysian prime minister Mahathir Mohamad said: "Today we, the whole Muslim *ummah* [community of believers] are treated with contempt and dishonour. Our religion is denigrated. Our holy places desecrated. Our countries are occupied. Our people are starved and killed. None of our countries are truly independent. We are under pressure to conform to our oppressors' wishes about how we should behave, how we should govern our lands, how we should think even." He added: "There is a feeling of hopelessness among the Muslim countries and their people. They feel that they can do nothing right. They believe that things can only get worse. The Muslims will forever be oppressed and dominated by the Europeans and Jews." The prime minister's argument was that the Muslims should gather their assets, not striking back blindly, but instead planning a thoughtful, long-term strategy to defeat their worldwide enemies, which he argued were controlled by the Jews. "But today the Jews rule the world by proxy. They get others to fight and die for them." Speech at the Opening of the Tenth Session of the Islamic Summit Conference, Oct. 16, 2003 (online at www.oicsummit2003.Org.my/speech_03.php).

5. CIA map, "Possible Remove Havens for Terrorist and Other Illicit Activity," May 2003.

6. For the numbers, see Tariq interview (Oct. 20, 2003).

7. For Pakistan playing a key role in apprehending 500 terrorists, see Richard Armitage testimony, Mar. 23, 2004.

8. For Pakistan's unpoliced areas, see Tasneem Noorani interview (Oct. 27, 2003).

9. Pakistanis and Afghanis interviews (Oct. 2003); DOD Special Operations Command and Central Command briefings (Sept. 15–16, 2004); U.S. intelligence official interview (July 9, 2004).

10. Pervez Musharraf. "A Plea for Enlightened Moderation: Muslims Must Raise Themselves Up Through Individual Achievement and Socioeconomic Emancipation," *Washington Post*, June 1, 2004, p. A23.

11. For a review of ISAF's role, see NATO report, "NATO in Afghanistan," updated July 9, 2004 (online at www.nato.int/issues/afghanistan).

12. United States Institute of Peace report, "Establishing the Rule of Law in Afghanistan," Mar. 2004, pp. 1–3 (online at www.usip.org/pubs/specialreports/sr117.html).

13. For the change, see Lakhdar Brahimi interview (Oct. 24, 2003); U.S. officials in Afghanistan interview (Oct. 2003). For the request that the United States remain, see Kandahar province local leaders interview (Oct. 21, 2003). For the effect of the United States leaving, see Karim Khalili interview (Oct. 23, 2003).

14. Some have criticized the Bush administration for neglecting Afghanistan because of Iraq. Others, including General Franks, say that the size of the U.S. military commitment in Afghanistan has not been compromised by the commitments in Iraq. We have not investigated the issue and cannot offer a judgment on it.

15. Even if the U.S. forces, stretched thin, are reluctant to take on this role, "a limited, but extremely useful, change in the military mandate would involve intelligence sharing with civilian law enforcement and a willingness to take action against drug warehouses and heroin laboratories." United States Institute of Peace report, "Establishing the Rule of Law in Afghanistan," Mar. 2004, p. 17.

16. For barriers to Saudi monitoring of charities, see, e.g., Robert Jordan interview (Jan. 14, 2004); David Aufhauser interview (Feb. 12, 2004).

17. For the Saudi reformer's view, see Members of *majles al-shura* interview (Oct. 14, 2003).

18. Neil MacFarquhar, "Saudis Support a Jihad in Iraq, Not Back Home," *New York Times*, Apr. 23, 2004, p. A1.

19. Prince Bandar Bin Sultan, "A Diplomat's Call for War," *Washington Post*, June 6, 2004, p. B4 (translation of original in *Al-Watan*, June 2, 2004).

20. President Clinton meeting (Apr. 8, 2004).

21. For Jordan's initiatives, see testimony of William Burns before the Subcommittee on the Middle East and Central Asia of the House International Relations Committee, Mar. 19, 2003 (online at www.house.gov/international_relations/108/burn0319.htm). For the report, see United Nations Development Programme report. *Arab Human Development Report 2003: Building a Knowledge Society* (United Nations, 2003) (online at www.miftah.org/Doc/Reports/Englishcomplete2003.pdf).

22. DOD memo, Rumsfeld to Myers, Wolfowitz, Pace, and Feith, "Global War on Terrorism." Oct. 16, 2003 (online at www.usatoday.com/news/washington/executive/rumsfeld-memo.htm).

23. For the statistics, see James Zogby, *What Arabs Think: Values, Beliefs, and Concerns* (Zogby International, 2002). For fear of a U.S. attack, see Pew Global Attitudes Project report, *Views of a Changing World: June 2003* (Pew Research Center for the People and the Press, 2003), p. 2. In our interviews, current and former U.S. officials dealing with the Middle East corroborated these findings.

24. For polling soon after 9/11, see Pew Research Center for the People and the Press report, "America Admired, Yet Its New Vulnerability Seen as Good Thing, Say Opinion Leaders; Little Support for Expanding War on Terrorism" (online at http://people-press.org/reports/print.php3?ReportID=145). For the quotation, see Pew Global Attitudes Project report, "War With Iraq Further Divides Global Publics But World Embraces Democratic Values and Free Markets," June 3, 2003 (online at www.pewtrusts.com/ideas/ideas_item.cfm?content_item_id=1645&content_type_id=7).

25. For the Occidentalist "creed of Islamist revolutionaries," see, e.g., Avishai Margalit and Ian Baruma, *Occidentalism: The West in the Eyes of Its Enemies* (Penguin Press, 2004).

26. We draw these statistics, significantly, from the U.S. government's working paper circulated in April 2004 to G-8 "sherpas" in preparation for the 2004 G-8 summit. The paper was leaked and published in *Al-Hayat*. "U.S. Working Paper for G-8 Sherpas," *Al-Hayat*, Feb. 13, 2004 (online at http://english.daralhayat.com/Spec/02-2004/Article-20040213-ac40bdaf-c0a8-01ed-004e-5e7ac897d678/story.html).

27. Richard Holbrooke, "Get the Message Out," *Washington Post*, Oct. 28, 2001, p. B7; Richard Armitage Interview (Jan. 12, 2004).

28. Testimony of George Tenet, "The Worldwide Threat 2004: Challenges in a Changing Global Context," before the Senate Select Committee on Intelligence, Feb. 24, 2004.

29. U.S. Department of Energy Advisory Board report, "A Report Card on the Department of Energy's Non-proliferation Programs with Russia," Jan. 10, 2001, p. vi.

30. For terrorists being self-funding, see United Nations report, "Second Report of the [UN] Monitoring Group, Pursuant to Security Council Resolution 1390," Sept. 19, 2002, p. 13.

31. For legal entry, see White House report, Office of Homeland Security, "The National Strategy for Homeland Security," July 2002, p. 20 (online at www.whitehouse.gov/homeland/book/index.html). For illegal entry, see Chicago Council on Foreign Relations task force report, *Keeping the Promise: Immigration Proposals from the Heartland* (Chicago Council on Foreign Relations, 2004), p. 28.

32. The names of at least three of the hijackers (Nawaf al Hazmi, Salem al Hazmi, and Khalid al Mihdhar) were in information systems of the intelligence community and thus potentially could have been watchlisted. Had they been watchlisted, the connections to terrorism could have been exposed at the time they applied for a visa or at the port of entry. The names of at least three of the hijackers (Nawaf al Hazmi, Salem al Hazmi, and Khalid al Mihdhar), were in information systems of the intelligence community and thus potentially could have been watchlisted. Had they been watchlisted, their terrorist affiliations could have been exposed either at the time they applied for a visa or at the port of entry. Two of the hijackers (Satam al Suqami and Abdul Aziz al Omari) presented passports manipulated in a fraudulent manner that has subsequently been associated with al Qaeda. Based on our review of their visa and travel histories, we believe it possible that as many as eleven additional hijackers (Wail al Shehri, Waleed al Shehri, Mohand al Shehri, Hani Hanjour, Majed Moqed, Nawaf al Hazmi, Hamza al Ghamdi, Ahmed al Ghamdi, Saeed al Ghamdi, Ahmed al Nami, and Ahmad al Haznawi) held passports containing these same fraudulent features, but their passports have not been found so we cannot be sure. Khalid al Mihdhar and Salem al Hazmi presented passports with a suspicious indicator of Islamic extremism. There is reason to believe that the passports of three other hijackers (Nawaf al Hazmi, Ahmed al Nami, and Ahmad al Haznawi) issued in the same Saudi passport office may have contained this same indicator; however, their passports have not been found, so we cannot be sure.

33. Khallad Bin Attash, Ramzi Binalshibh, Zakariya Essabar, Ali Abdul Aziz Ali, and Saeed al Ghamdi (not the individual by the same name who became a hijacker) tried to get visas and failed. Kahtani was unable to prove his admissibility and withdrew his application for admission after an immigration inspector remained unpersuaded that he was a tourist. All the hijackers whose visa applications we reviewed arguably could have been denied visas because their applications were not filled out completely. Had State visa officials routinely had a practice of acquiring more information in such cases, they likely would have found more grounds for denial. For example, three hijackers made statements on their visa applications that could have been proved false by U.S. government records (Hani Hanjour, Saeed al Ghamdi, and Khalid al Mihdhar), and many lied about their employment or educational status. Two hijackers could have been denied admission at the port of entry based on violations of immigration rules governing terms of admission—Mohamed Atta overstayed his tourist visa and then failed to present a proper vocational school visa when he entered in January 2001: Ziad Jarrah attended school in June 2000 without properly adjusting his immigration status, an action that violated his immigration status and rendered him inadmissible on each of his six subsequent reentries into the United States between June 2000 and August 5, 2001. There were possible grounds to deny entry to a third hijacker (Marwan al Shehhi). One hijacker violated his immigration status by failing to enroll as a student after entry (Hani Hanjour); two hijackers overstayed their terms of admission by four and eight months respectively (Satam al Suqami and Nawaf al Hazmi). Atta and Shehhi attended a flight school (Huffman Aviation) that the Justice Department's Inspector General concluded should not have been certified to accept foreign students, see DOJ Inspector General's report, "The INS' Contacts with Two September 11 Terrorists: A Review of the INS's Admissions of Atta and Shehhi, its Processing of their Change of Status Applications, and its Efforts to Track Foreign Students in the United States," May 20, 2002.

34. John Gordon interview (May 13, 2004).

35. For a description of a layering approach, see Stephen Flynn, *American the Vulnerable: How the U.S. Has Failed to Secure the Homeland and Protect Its People from Terrorism* (HarperCollins, 2004), p. 69.

36. The logical and timely rollout of such a program is hampered by an astonishingly long list of congressional mandates. The system originated in the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 and applied to all non-U.S. citizens who enter or exit the United States at any port of entry. Pub. L. No. 104–208, 110 Stat. 3009 (1996), § 110. The Data Management Improvement Act of 2000 altered this mandate by incorporating a requirement for a searchable centralized database, limiting the government's ability to require new data from certain travelers and setting a series of implementation deadlines. Pub. L. No. 106–215, 114 Stat. 337 (2000), § 2(a). The USA PATRIOT Act mandated that the Attorney General and Secretary of State "particularly focus" on having the entry-exit system include biometrics and tamper-resistant travel documents readable at all ports of entry. Pub. L. No. 107–56, 115 Stat. 272 (2001), § 1008(a). In the Enhanced Border Security and Visa Entry Reform Act, Congress directed that, not later than October 26, 2004, the attorney general and the secretary of state issue to all non-U.S. citizens only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers and install equipment at all U.S. ports of entry to allow biometric authentication of such documents. Pub. L. No. 107–173, 116 Stat. 543 (2002), § 303(b). The Act also required that increased security still facilitate the free flow of commerce and travel. Ibid. § 102(a)(1)(C). The administration has requested a delay of two years for the requirement of tamper-proof passports. Testimony of Thomas Ridge before the House Judiciary Committee, Apr. 21, 2004 (online at www.dhs.gov/dhspublic/display?theme=45&content=3498&print=true). Program planners have set a goal of collecting information, confirming identity, providing information about foreign nationals throughout the entire immigration system, and ultimately enabling each point in the system to assess the lawfulness of travel and any security risks.

37. There are at least three registered traveler programs underway, at different points in the system, designed and run by two different agencies in the Department of Homeland Security (outside the U.S.VISIT system), which must ultimately be the basis for access to the United States.

38. For the statistics, see DOS report, "Workload Statistics by Post Regions for All Visa Classes" June 18, 2004. One post-9/11 screening process, known as Condor, has conducted over 130,000 extra name-checks. DOS letter, Karl Hofmann to the Commission, Apr. 5, 2004. The checks have caused significant delays in some cases but have never resulted in visas being denied on terrorism grounds. For a discussion of visa delays, see General Accounting Office report, "Border Security: Improvements Needed to Reduce Time Taken to Adjudicate Visas for Science Students and Scholars," Feb. 2004. We do not know all the reasons why visa applications have dropped so significantly. Several factors beyond the visa process itself include the National Security Entry-Exit Registration System, which requires additional screening processes for certain groups from Arab and Muslim countries; the Iraq war; and perhaps cyclical economic factors. For the cost to the United States of visa backlogs, see National Foreign Trade Council report, "Visa Backlog Costs U.S. Exporters More than $30 Billion Since 2002, New Study Finds," June 2, 2004 (online at www.nftc.org/newsflash/newsflash.asp?Mode=View&articleid=1686&Category=All).

39. These issues are on the G-8 agenda. White House press release, "G-8 Secure and Facilitated Travel Initiative (SAFTI)," June 9, 2004 (online at www.whitehouse.gov/news/releases/2004/06/20040609-51.html). Lax passport issuance standards are among the vulnerabilities exploited by terrorists, possibly including two of the 9/11 hijackers. Three models exist for strengthened prescreening: (1) better screening by airlines, such as the use of improved document authentication technology: (2) posting of border agents or inspectors in foreign airports to work cooperatively with foreign counterparts; and (3) establishing a full preinspection regime, such as now exists for travel to the United States from Canada and Ireland. All three models should be pursued, in addition to electronic prescreening.

40. Among the more important problems to address is that of varying transliterations of the same name. For example, the current lack of a single convention for transliterating Arabic names enabled the 19 hijackers to vary the spelling of their names to defeat name-based watchlist systems and confuse any potential efforts to locate them. While the gradual introduction of biometric identifiers will help, that process will take years, and a name match will always be useful. The ICAO

should discuss the adoption of a standard requiring a digital code for all names that need to be translated into the Roman alphabet, ensuring one common spelling for all countries.

41. On achieving more reliable identification, see Markle Foundation task force report, *Creating a Trusted Information Network for Homeland Security* (Markle Foundation, 2003), p. 72 (online at www.markle.org).

42. General Accounting Office report, *Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges*, GAO-03-263, Dec. 2002 (online at www.gao.gov/new.items/d03263.pdf).

13 HOW TO DO IT? A DIFFERENT WAY OF ORGANIZING THE GOVERNMENT

As presently configured, the national security institutions of the U.S. government are still the institutions constructed to win the Cold War. The United States confronts a very different world today. Instead of facing a few very dangerous adversaries, the United States confronts a number of less visible challenges that surpass the boundaries of traditional nation-states and call for quick, imaginative, and agile responses.

The men and women of the World War II generation rose to the challenges of the 1940s and 1950s. They restructured the government so that it could protect the country. That is now the job of the generation that experienced 9/11. Those attacks showed, emphatically, that ways of doing business rooted in a different era are just not good enough. Americans should not settle for incremental, ad hoc adjustments to a system designed generations ago for a world that no longer exists.

We recommend significant changes in the organization of the government. We know that the quality of the people is more important than the quality of the wiring diagrams. Some of the saddest aspects of the 9/11 story are the outstanding efforts of so many individual officials straining, often without success, against the boundaries of the possible. Good people can overcome bad structures. They should not have to.

The United States has the resources and the people. The government should combine them more effectively, achieving unity of effort. We offer five major recommendations to do that:

- unifying strategic intelligence and operational planning against Islamist terrorists across the foreign-domestic divide with a National Counterterrorism Center;
- unifying the intelligence community with a new National Intelligence Director;
- unifying the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional governmental boundaries;
- unifying and strengthening congressional oversight to improve quality and accountability; and
- strengthening the FBI and homeland defenders.

13.1 UNITY OF EFFORT ACROSS THE FOREIGN-DOMESTIC DIVIDE

Joint Action

Much of the public commentary about the 9/11 attacks has dealt with "lost opportunities," some of which we reviewed in chapter 11. These are often characterized as problems of "watchlisting," of "information sharing," or of "connecting the dots." In chapter 11 we explained that these labels are too narrow. They describe the symptoms, not the disease.

In each of our examples, no one was firmly in charge of managing the case and able to draw relevant intelligence from anywhere in the government, assign responsibilities across the agencies (foreign or domestic), track progress, and quickly bring obstacles up to the level where they could be resolved. Responsibility and accountability were diffuse.

The agencies cooperated, some of the time. But even such cooperation as there was is not the same thing as joint action. When agencies cooperate, one defines the problem and seeks help with it. When they act jointly, the problem and options for action are defined differently from the start. Individuals from different backgrounds come together in analyzing a case and planning how to manage it.

In our hearings we regularly asked witnesses: Who is the quarterback? The other players are in their positions, doing their jobs. But who is calling the play that assigns roles to help them execute as a team?

Since 9/11, those issues have not been resolved. In some ways joint work has gotten better, and in some ways worse. The effort of fighting terrorism has flooded over many of the usual agency boundaries because of its sheer quantity and energy. Attitudes have changed. Officials are keenly conscious of trying to avoid the mistakes of 9/11. They try to share information. They circulate—even to the President—practically every reported threat, however dubious.

Partly because of all this effort, the challenge of coordinating it has multiplied. Before 9/11, the CIA was plainly the lead agency confronting al Qaeda. The FBI played a very secondary role. The engagement of the departments of Defense and State was more episodic.

- Today the CIA is still central. But the FBI is much more active, along with other parts of the Justice Department.
- The Defense Department effort is now enormous. Three of its unified commands, each headed by a four-star general, have counterterrorism as a primary mission: Special Operations Command, Central Command (both headquartered in Florida), and Northern Command (headquartered in Colorado).
- A new Department of Homeland Security combines formidable resources in border and transportation security, along with analysis of domestic vulnerability and other tasks.
- The State Department has the lead on many of the foreign policy tasks we described in chapter 12.
- At the White House, the National Security Council (NSC) now is joined by a parallel presidential advisory structure, fhe Homeland Security Council.

So far we have mentioned two reasons for joint action—the virtue of joint planning and the advantage of having someone in charge to ensure a unified effort. There is a third: the simple shortage of experts with sufficient skills. The limited pool of critical experts—for example, skilled counterterrorism analysts and linguists—is being depleted. Expanding these capabilities will require not just money, but time.

Primary responsibility for terrorism analysis has been assigned to the Terrorist Threat Integration Center (TTIC), created in 2003, based at the CIA headquarters but staffed with representatives of many agencies, reporting directly to the Director of Central Intelligence. Yet the CIA houses another intelligence "fusion" center: the Counterterrorist Center that played such a key role before 9/11. A third major analytic unit is at Defense, in the Defense Intelligence Agency. A fourth, concentrating more on homeland vulnerabilities, is at the Department of Homeland Security. The FBI is in the process of building the analytic capability it has long lacked, and it also has the Terrorist Screening Center.[1]

The U.S. government cannot afford so much duplication of effort. There are not enough experienced experts to go around. The duplication also places extra demands on already hard-pressed single-source national technical intelligence collectors like the National Security Agency.

Combining Joint Intelligence and Joint Action

A "smart" government would *integrate* all sources of information to see the enemy as a whole. Integrated all-source analysis should also inform and shape strategies to collect more intelligence. Yet the Terrorist Threat Integration Center, while it has primary responsibility for terrorism analysis, is formally proscribed from having any oversight or operational authority and is not part of any operational entity, other than reporting to the director of central intelligence.[2]

The government now tries to handle the problem of joint management, informed by analysis of intelligence from all sources, in two ways.

- First, agencies with lead responsibility for certain problems have constructed their own interagency entities and task forces in order to get cooperation. The Counterterrorist Center at CIA, for example, recruits liaison officers from throughout the intelligence community. The military's Central Command has its own interagency center, recruiting liaison officers from all the agencies from which it might need help. The FBI has joint Terrorism Task Forces in 84 locations to coordinate the activities of other agencies when action may be required.
- Second, the problem of joint operational planning is often passed to the White House, where the NSC staff tries to play this role. The national security staff at the White House (both NSC and new Homeland Security Council staff) has already become 50 percent larger since 9/11. But our impression, after talking to serving officials, is that even this enlarged staff is consumed by meetings on day-to-day issues, sifting each day's threat information and trying to coordinate everyday operations.

Even as it crowds into every square inch of available office space, the NSC staff is still not sized or funded to be an executive agency. In chapter 3 we described some of the problems that arose in the 1980s when a White House staff, constitutionally insulated from the usual mechanisms of oversight, became involved in direct operations. During the 1990s Richard Clarke occasionally tried to exercise such authority, sometimes successfully, but often causing friction.

Yet a subtler and more serious danger is that as the NSC staff is consumed by these day-to-day tasks, it has less capacity to find the time and detachment needed to advise a president on larger policy issues. That means less time to work on major new initiatives, help with legislative management to steer needed bills through Congress, and track the design and implementation of the strategic plans for regions, countries, and issues that we discuss in chapter 12.

Much of the job of operational coordination remains with the agencies, especially the CIA. There DCI Tenet and his chief aides ran interagency meetings nearly every day to coordinate much of the government's day-to-day work. The DCI insisted he did not make policy and only oversaw its implementation. In the struggle against terrorism these distinctions seem increasingly artificial. Also, as the DCI becomes a lead coordinator of the

government's operations, it becomes harder to play all the position's other roles, including that of analyst in chief.

The problem is nearly intractable because of the way the government is currently structured. Lines of operational authority run to the expanding executive departments, and they are guarded for understandable reasons: the DCI commands the CIA's personnel overseas; the secretary of defense will not yield to others in conveying commands to military forces; the justice Department will not give up the responsibility of deciding whether to seek arrest warrants. But the result is that each agency or department needs its own intelligence apparatus to support the performance of its duties. It is hard to "break down stovepipes" when there are so many stoves that are legally and politically entitled to have cast-iron pipes of their own.

Recalling the Goldwater-Nichols legislation of 1986, Secretary Rumsfeld reminded us that to achieve better joint capability, each of the armed services had to "give up some of their turf and authorities and prerogatives." Today, he said, the executive branch is "stovepiped much like the four services were nearly 20 years ago." He wondered if it might be appropriate to ask agencies to "give up some of their existing turf and authority in exchange for a stronger, faster, more efficient government wide joint effort."[3] Privately, other key officials have made the same point to us.

We therefore propose a new institution: a civilian-led unified joint command for counterterrorism. It should combine strategic intelligence and joint operational planning.

In the Pentagon's Joint Staff, which serves the chairman of the joint Chiefs of Staff, intelligence is handled by the J-2 directorate, operational planning by J-3, and overall policy by J-5. Our concept combines the J-2 and J-3 functions (intelligence and operational planning) in one agency, keeping overall policy coordination where it belongs, in the National Security Council.

Recommendation: We recommend the establishment of a National Counterterrorism Center (NCTC), built on the foundation of the existing Terrorist Threat Integration Center (TTIC). Breaking the older mold of national government organization, this NCTC should be a center for joint operational planning *and* joint intelligence, staffed by personnel from the various agencies. The head of the NCTC should have authority to evaluate the performance of the people assigned to the Center.

- Such a joint center should be developed in the same spirit that guided the military's creation of unified joint commands, or the shaping of earlier national agencies like the National Reconnaissance Office, which was formed to organize the work of the CIA and several defense agencies in space.

  NCTC—Intelligence. The NCTC should lead strategic analysis, pooling all-source intelligence, foreign and domestic, about transnational terrorist organizations with global reach. It should develop *net* assessments (comparing enemy capabilities and intentions against U.S. defenses and countermeasures). It should also provide warning. It should do this work by drawing on the efforts of the CIA, FBI, Homeland Security, and other departments and agencies. It should task collection requirements both inside and outside the United States.
- The intelligence function (J-2) should build on the existing TTIC structure and remain distinct, as a national intelligence center, within the NCTC. As the government's principal knowledge bank on Islamist terrorism, with the main responsibility for strategic analysis and net assessment, it should absorb a significant

portion of the analytical talent now residing in the CIA's Counterterrorist Center and the DIA's Joint Intelligence Task Force—Combatting Terrorism (JITF-CT).

NCTC—Operations. The NCTC should perform joint planning. The plans would assign operational responsibilities to lead agencies, such as State, the CIA, the FBI, Defense and its combatant commands, Homeland Security, and other agencies. The NCTC should *not* direct the actual execution of these operations, leaving that job to the agencies. The NCTC would then track implementation; it would look across the foreign-domestic divide and across agency boundaries, updating plans to follow through on cases.[4]

- The joint operational planning function (J-3) will be new to the TTIC structure. The NCTC can draw on analogous work now being done in the CIA and every other involved department of the government, as well as reaching out to knowledgeable officials in state and local agencies throughout the United States.
- The NCTC should *not* be a policymaking body. Its operations and planning should follow the policy direction of the president and the National Security Council.

Consider this hypothetical case. The NSA discovers that a suspected terrorist is traveling to Bangkok and Kuala Lumpur. The NCTC should draw on joint intelligence resources, including its own NSA counterterrorism experts, to analyze the identities and possible destinations of these individuals. Informed by this analysis, the NCTC would then organize and plan the management of the case, drawing on the talents and differing kinds of experience among the several agency representatives assigned to it—assigning tasks to the CIA overseas, to Homeland Security watching entry points into the United States, and to the FBI. If military assistance might be needed, the Special Operations Command could be asked to develop an appropriate concept for such an operation. The NCTC would be accountable for tracking the progress of the case, ensuring that the plan evolved with it, and integrating the information into a warning. The NCTC would be responsible for being sure that intelligence gathered from the activities in the field became part of the government's institutional memory about Islamist terrorist personalities, organizations, and possible means of attack.

In each case the involved agency would make its own senior managers aware of what it was being asked to do. If those agency heads objected, and the issue could not easily be resolved, then the disagreement about roles and missions could be brought before the National Security Council and the president.

NCTC—Authorities. The head of the NCTC should be appointed by the president, and should be equivalent in rank to a deputy head of a cabinet department. The head of the NCTC would report to the national intelligence director, an office whose creation we recommend below, placed in the Executive Office of the President. The head of the NCTC would thus also report indirectly to the president. This official's nomination should be confirmed by the Senate and he or she should testify to the Congress, as is the case now with other statutory presidential offices, like the U.S. trade representative.

- To avoid the fate of other entities with great nominal authority and little real power, the head of the NCTC must have the right to concur in the choices of personnel to lead the operating entities of the departments and agencies focused on counterterrorism, specifically including the head of the Counterterrorist Center, the head of the FBI's Counterterrorism Division, the commanders of the Defense Department's Special Operations Command and Northern Command, and the State Department's coordinator for counterterrorism.[5] The head of the NCTC should also work with the director of the Office of Management and Budget in developing the president's counterterrorism budget.
- There are precedents for surrendering authority for joint planning while preserving an agency's operational control. In the international context, NATO commanders may get line authority over forces assigned by other nations. In U.S. unified commands, commanders plan operations that may involve units belonging to one of the services. In each case, procedures are worked out, formal and informal, to define the limits of the joint commander's authority.

The most serious disadvantage of the NCTC is the reverse of its greatest virtue. The struggle against Islamist terrorism is so important that any clear-cut centralization of authority to manage and be accountable for it may concentrate too much power in one place. The proposed NCTC would be given the authority of planning the activities of other agencies. Law or executive order must define the scope of such line authority.

The NCTC would not eliminate interagency policy disputes. These would still go to the National Security Council. To improve coordination at the White House, we believe the existing Homeland Security Council should soon be merged into a single National Security Council. The creation of the NCTC should help the NSC staff concentrate on its core duties of assisting the president and supporting interdepartmental policymaking.

We recognize that this is a new and difficult idea precisely because the authorities we recommend for the NCTC really would, as Secretary Rumsfeld foresaw, ask strong agencies to "give up some of their turf and authority in exchange for a stronger, faster, more efficient government wide joint effort." Countering transnational Islamist terrorism will test whether the U.S. government can fashion more flexible models of management needed to deal with the twenty-first-century world.

An argument against change is that the nation is at war, and cannot afford to reorganize in midstream. But some of the main innovations of the 1940s and 1950s, including the creation of the Joint Chiefs of Staff and even the construction of the Pentagon itself, were undertaken in the midst of war. Surely the country cannot wait until the struggle against Islamist terrorism is over.

"Surprise, when it happens to a government, is likely to be a complicated, diffuse, bureaucratic thing. It includes neglect of responsibility, but also responsibility so poorly defined or so ambiguously delegated that action gets lost."[6] That comment was made more than 40 years ago, about Pearl Harbor. We hope another commission, writing in the future about another attack, does not again find this quotation to be so apt.

13.2 UNITY OF EFFORT IN THE INTELLIGENCE COMMUNITY

In our first section, we concentrated on counterterrorism, discussing how to combine the analysis of information from all sources of intelligence with the joint planning of operations that draw on that analysis. In this section, we step back from looking just at the

counterterrorism problem. We reflect on whether the government is organized adequately to direct resources and build the intelligence capabilities it will need not just for countering terrorism, but for the broader range of national security challenges in the decades ahead.

The Need for a Change

During the Cold War, intelligence agencies did not depend on seamless integration to track and count the thousands of military targets—such as tanks and missiles—fielded by the Soviet Union and other adversary states. Each agency concentrated on its specialized mission, acquiring its own information and then sharing it via formal, finished reports. The Department of Defense had given birth to and dominated the main agencies for technical collection of intelligence. Resources were shifted at an incremental pace, coping with challenges that arose over years, even decades.

We summarized the resulting organization of the intelligence community in chapter 3. It is outlined below.

Members of the U.S. Intelligence Community

Office of the Director of Central Intelligence, which includes the Office of the Deputy Director of Central Intelligence for Community Management, the Community Management Staff, the Terrorism Threat Integration Center, the National Intelligence Council, and other community offices

The Central Intelligence Agency (CIA), which performs human source collection, all-source analysis, and advanced science and technology

National intelligence agencies:

- National Security Agency (NSA), which performs signals collection and analysis
- National Geospatial-Intelligence Agency (NGA), which performs imagery collection and analysis
- National Reconnaissance Office (NRO), which develops, acquires, and launches space systems for intelligence collection
- Other national reconnaissance programs

Departmental intelligence agencies:

- Defense Intelligence Agency (DIA) of the Department of Defense
- Intelligence entities of the Army, Navy, Air Force, and Marines
- Bureau of Intelligence and Research (INR) of the Department of State
- Office of Terrorism and Finance Intelligence of the Department of Treasury
- Office of Intelligence and the Counterterrorism and Counterintelligence Divisions of the Federal Bureau of Investigation of the Department of Justice
- Office of Intelligence of the Department of Energy
- Directorate of Information Analysis and Infrastructure Protection (IAIP) and Directorate of Coast Guard Intelligence of the Department of Homeland Security

The need to restructure the intelligence community grows out of six problems that have become apparent before and after 9/11:

- *Structural barriers to performing joint intelligence work.* National intelligence is still organized around the collection disciplines of the home agencies, not the joint mission. The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots." No one component holds all the relevant information.By contrast, in organizing national defense, the Goldwater-Nichols legislation of 1986 created joint commands for operations in the field, the Unified Command Plan. The services—the Army, Navy, Air Force, and Marine Corps—organize, train, and equip their people and units to perform their missions. Then they assign personnel and units to the joint combatant commander, like the commanding general of the Central Command (CENTCOM). The Goldwater-Nichols Act required officers to serve tours outside their service in order to win promotion. The culture of the Defense Department was transformed, its collective mind-set moved from service-specific to 'joint," and its operations became more integrated.[7]
- *Lack of common standards and practices across the foreign-domestic divide. The* leadership of the intelligence community should be able to pool information gathered overseas with information gathered in the United States, holding the work—wherever it is done—to a common standard of quality in how it is collected, processed (e.g., translated), reported, shared, and analyzed. A common set of personnel standards for intelligence can create a group of professionals better able to operate in joint activities, transcending their own service-specific mind-sets.
- *Divided management of national intelligence capabilities.* While the CIA was once "central" to our national intelligence capabilities, following the end of the Cold War it has been less able to influence the use of the nation's imagery and signals intelligence capabilities in three national agencies housed within the Department of Defense: the National Security Agency, the National Geospatial-Intelligence Agency, and the National Reconnaissance Office. One of the lessons learned from the 1991 Gulf War was the value of national intelligence systems (satellites in particular) in precision warfare. Since that war, the department has appropriately drawn these agencies into its transformation of the military. Helping to orchestrate this transformation is the under secretary of defense for intelligence, a position established by Congress after 9/11. An unintended consequence of these developments has been the far greater demand made by Defense on technical systems, leaving the DCI less able to influence how these technical resources are allocated and used.
- *Weak capacity to set priorities and move resources.* The agencies are mainly organized around what they collect or the way they collect it. But the priorities for collection are national. As the DCI makes hard choices about moving resources, he or she must have the power to reach across agencies and reallocate effort.
- *Too many jobs.* The DCI now has at least three jobs. He is expected to run a particular agency, the CIA. He is expected to manage the loose confederation of agencies that is the intelligence community. He is expected to be the analyst in chief for the government, sifting evidence and directly briefing the President as his principal intelligence adviser. No recent DCI has been able to do all three effectively. Usually what loses out is management of the intelligence community, a

difficult task even in the best case because the DCI's current authorities are weak. With so much to do, the DCI often has not used even the authority he has.

- *Too complex and secret.* Over the decades, the agencies and the rules surrounding the intelligence community have accumulated to a depth that practically defies public comprehension. There are now 15 agencies or parts of agencies in the intelligence community. The community and the DCI's authorities have become arcane matters, understood only by initiates after long study. Even the most basic information about how much money is actually allocated to or within the intelligence community and most of its key components is shrouded from public view.

The current DCI is responsible for community performance but lacks the three authorities critical for any agency head or chief executive officer: (1) control over purse strings, (2) the ability to hire or fire senior managers, and (3) the ability to set standards for the information infrastructure and personnel.[8]

The only budget power of the DCI over agencies other than the CIA lies in coordinating the budget requests of the various intelligence agencies into a single program for submission to Congress. The overall funding request of the 15 intelligence entities in this program is then presented to the president and Congress in 15 separate volumes.

When Congress passes an appropriations bill to allocate money to intelligence agencies, most of their funding is hidden in the Defense Department in order to keep intelligence spending secret. Therefore, although the House and Senate Intelligence committees are the authorizing committees for funding of the intelligence community, the final budget review is handled in the Defense Subcommittee of the Appropriations committees. Those committees have no subcommittees just for intelligence, and only a few members and staff review the requests.

The appropriations for the CIA and the national intelligence agencies—NSA, NGA, and NRO—are then given to the secretary of defense. The secretary transfers the CIA's money to the DCI but disburses the national agencies' money directly. Money for the FBI's national security components falls within the appropriations for Commerce, Justice, and State and goes to the attorney general.[9]

In addition, the DCI lacks hire-and-fire authority over most of the intelligence community's senior managers. For the national intelligence agencies housed in the Defense Department, the secretary of defense must seek the DCI's concurrence regarding the nomination of these directors, who are presidentially appointed. But the secretary may submit recommendations to the president without receiving this concurrence. The DCI cannot fire these officials. The DCI has even less influence over the head of the FBI's national security component, who is appointed by the attorney general in consultation with the DCI.[10]

Combining Joint Work with Stronger Management

We have received recommendations on the topic of intelligence reform from many sources. Other commissions have been over this same ground. Thoughtful bills have been introduced, most recently a bill by the chairman of the House Intelligence Committee Porter Goss (R-Fla.), and another by the ranking minority member, Jane Harman (D-Calif.). In the Senate, Senators Bob Graham (D-Fla.) and Dianne Feinstein (D-Calif.) have introduced reform proposals as well. Past efforts have foundered, because the president did not support them; because the DCI, the secretary of defense, or both opposed them; and because some

proposals lacked merit. We have tried to take stock of these experiences, and borrow from strong elements in many of the ideas that have already been developed by others.

Recommendation: The current position of Director of Central Intelligence should be replaced by a National Intelligence Director with two main areas of responsibility: (1) to oversee national intelligence centers on specific subjects of interest across the U.S. government and (2) to manage the national intelligence program and oversee the agencies that contribute to it.

First, the National Intelligence Director should oversee *national intelligence centers* to provide all-source analysis and plan intelligence operations for the whole government on major problems.

- One such problem is counterterrorism. In this case, we believe that the center should be the intelligence entity (formerly TTIC) inside the National Counterterrorism Center we have proposed. It would sit there alongside the operations management unit we described earlier, with both making up the NCTC, in the Executive Office of the President. Other national intelligence centers—for instance, on counterproliferation, crime and narcotics, and China—would be housed in whatever department or agency is best suited for them.
- The National Intelligence Director would retain the present DCI's role as the principal intelligence adviser to the president. We hope the president will come to look directly to the directors of the national intelligence centers to provide all-source analysis in their areas of responsibility, balancing the advice of these intelligence chiefs against the contrasting viewpoints that may be offered by department heads at State, Defense, Homeland Security, Justice, and other agencies.

Second, the National Intelligence Director should manage the national intelligence program and oversee the component agencies of the intelligence community. (See diagram.)[11]

- The National Intelligence Director would submit a unified budget for national intelligence that reflects priorities chosen by the National Security Council, an appropriate balance among the varieties of technical and human intelligence collection, and analysis. He or she would receive an appropriation for national intelligence and apportion the funds to the appropriate agencies, in line with that budget, and with authority to reprogram funds among the national intelligence agencies to meet any new priority (as counterterrorism was in the 1990s). The National Intelligence Director should approve and submit nominations to the president of the individuals who would lead the CIA, DIA, FBI Intelligence Office, NSA, NGA, NRO, Information Analysis and Infrastructure Protection Directorate of the Department of Homeland Security, and other national intelligence capabilities.[12]
- The National Intelligence Director would manage this national effort with the help of three deputies, each of whom would also hold a key position in one of the component agencies.[13]
  - foreign intelligence (the head of the CIA)
  - defense intelligence (the under secretary of defense for intelligence)[14]
  - homeland intelligence (the FBI's executive assistant director for intelligence or the under secretary of homeland security for information analysis and infrastructure protection)

Other agencies in the intelligence community would coordinate their work within each of these three areas, largely staying housed in the same departments or agencies that support them now.

Returning to the analogy of the Defense Department's organization, these three deputies—like the leaders of the Army, Navy, Air Force, or Marines—would have the job of acquiring the systems, training the people, and executing the operations planned by the national intelligence centers.

And, just as the combatant commanders also report to the secretary of defense, the directors of the national intelligence centers—e.g., for counterproliferation, crime and narcotics, and the rest—also would report to the National Intelligence Director.

- The Defense Department's military intelligence programs—the joint military intelligence program (JMIP) and the tactical intelligence and related activities program (TIARA)—would remain part of that department's responsibility.
- The National Intelligence Director would set personnel policies to establish standards for education and training and facilitate assignments at the national intelligence centers and across agency lines. The National Intelligence Director also would set information sharing and information technology policies to maximize data sharing, as well as policies to protect the security of information.
- Too many agencies now have an opportunity to say no to change. The National Intelligence Director should participate in an NSC executive committee that can resolve differences in priorities among the agencies and bring the major disputes to the president for decision.

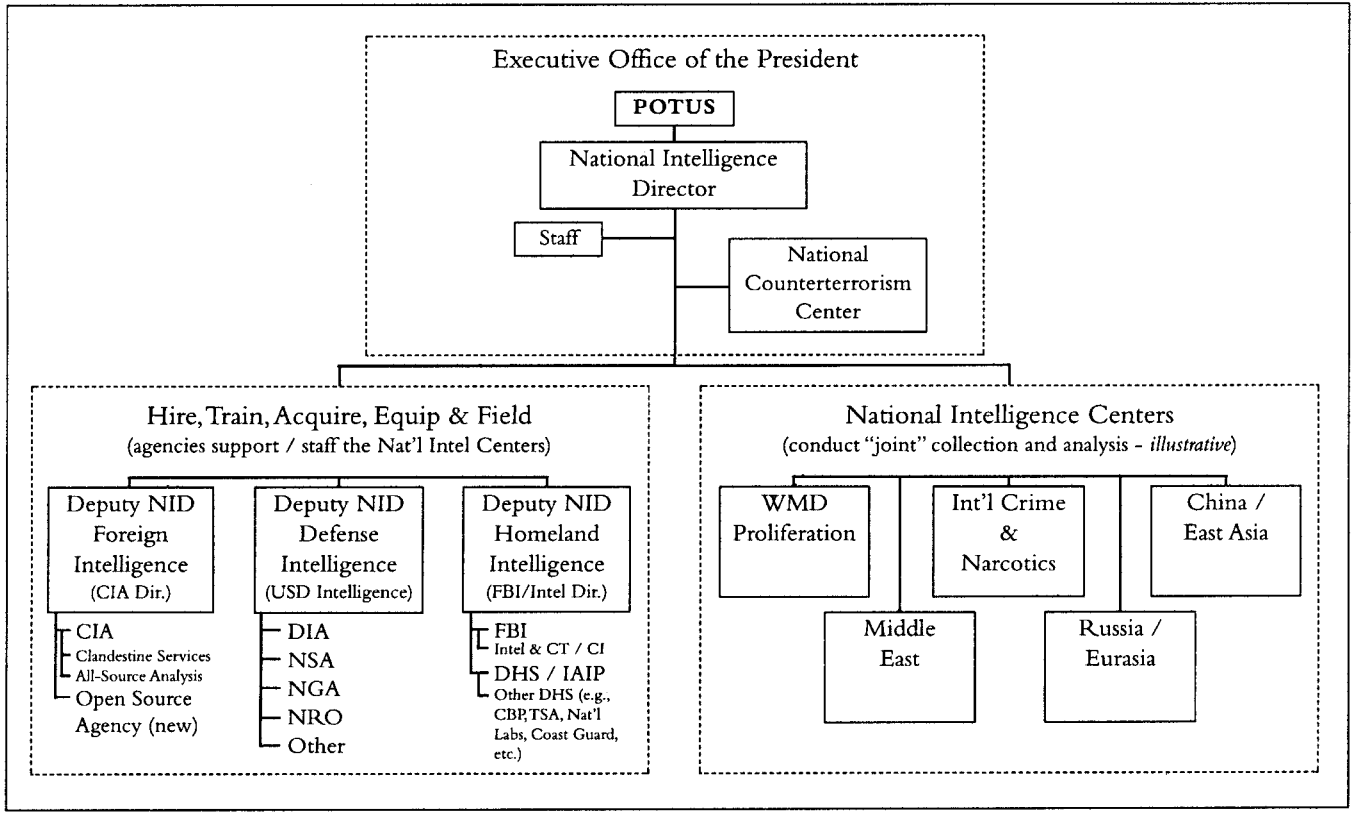
The National Intelligence Director should be located in the Executive Office of the President. This official, who would be confirmed by the Senate and would testify before Congress, would have a relatively small staff of several hundred people, taking the place of the existing community management offices housed at the CIA.

In managing the whole community, the National Intelligence Director is still providing a service function. With the partial exception of his or her responsibilities for overseeing the NCTC, the National Intelligence Director should support the consumers of national intelligence—the president and policymaking advisers such as the secretaries of state, defense, and homeland security and the attorney general.

We are wary of too easily equating government management problems with those of the private sector. But we have noticed that some very large private firms rely on a powerful CEO who has significant control over how money is spent and can hire or fire leaders of the major divisions, assisted by a relatively modest staff, while leaving responsibility for execution in the operating divisions.

There are disadvantages to separating the position of National Intelligence Director from the job of heading the CIA. For example, the National Intelligence Director will not head a major agency of his or her own and may have a weaker base of support. But we believe that these disadvantages are outweighed by several other considerations:

- The National Intelligence Director must be able to directly oversee intelligence collection inside the United States. Yet law and custom has counseled against giving such a plain domestic role to the head of the CIA.



Unity of Effort in Managing Intelligence

- The CIA will be one among several claimants for funds in setting national priorities. The National Intelligence Director should not be both one of the advocates and the judge of them all.
- Covert operations tend to be highly tactical, requiring close attention. The National Intelligence Director should rely on the relevant joint mission center to oversee these details, helping to coordinate closely with the White House. The CIA will be able to concentrate on building the capabilities to carry out such operations and on providing the personnel who will be directing and executing such operations in the field.
- Rebuilding the analytic and human intelligence collection capabilities of the CIA should be a full-time effort, and the director of the CIA should focus on extending its comparative advantages.

Recommendation: The CIA Director should emphasize (a) rebuilding the CIA's analytic capabilities; (b) transforming the clandestine service by building its human intelligence capabilities; (c) developing a stronger language program, with high standards and sufficient financial incentives; (d) renewing emphasis on recruiting diversity among operations officers so they can blend more easily in foreign cities; (e) ensuring a seamless relationship between human source collection and signals collection at the operational level; and (f) stressing a better balance between unilateral and liaison operations.

The CIA should retain responsibility for the direction and execution of clandestine and covert operations, as assigned by the relevant national intelligence center and authorized by the National Intelligence Director and the president. This would include propaganda, renditions, and nonmilitary disruption. We believe, however, that one important area of responsibility should change.

Recommendation: Lead responsibility for directing and executing paramilitary operations, whether clandestine or covert, should shift to the Defense Department. There it should be consolidated with the capabilities for training, direction, and execution of such operations already being developed in the Special Operations Command.

- Before 9/11, the CIA did not invest in developing a robust capability to conduct paramilitary operations with U.S. personnel. It relied on proxies instead, organized by CIA operatives without the requisite military training. The results were unsatisfactory.
- Whether the price is measured in either money or people, the United States cannot afford to build two separate capabilities for carrying out secret military operations, secretly operating standoff missiles, and secretly training foreign military or paramilitary forces. The United States should concentrate responsibility and necessary legal authorities in one entity.
- The post-9/11 Afghanistan precedent of using joint CIA-military teams for covert and clandestine operations was a good one. We believe this proposal to be consistent with it. Each agency would concentrate on its comparative advantages in building capabilities for joint missions. The operation itself would be planned in common.
- The CIA has a reputation for agility in operations. The military has a reputation for being methodical and cumbersome. We do not know if these stereotypes match current reality; they may also be one more symptom of the civil-military

misunderstandings we described in chapter 4. It is a problem to be resolved in policy guidance and agency management, not in the creation of redundant, overlapping capabilities and authorities in such sensitive work. The CIA's experts should be integrated into the military's training, exercises, and planning. To quote a CIA official now serving in the field: "One fight, one team."

Recommendation: Finally, to combat the secrecy and complexity we have described, the overall amounts of money being appropriated for national intelligence and to its component agencies should no longer be kept secret. Congress should pass a separate appropriations act for intelligence, defending the broad allocation of how these tens of billions of dollars have been assigned among the varieties of intelligence work.

The specifics of the intelligence appropriation would remain classified, as they are today. Opponents of declassification argue that America's enemies could learn about intelligence capabilities by tracking the top-line appropriations figure. Yet the top-line figure by itself provides little insight into U.S. intelligence sources and methods. The U.S. government readily provides copious information about spending on its military forces, including military intelligence. The intelligence community should not be subject to that much disclosure. But when even aggregate categorical numbers remain hidden, it is hard to judge priorities and foster accountability.

13.3 UNITY OF EFFORT IN SHARING INFORMATION

Information Sharing

We have already stressed the importance of intelligence analysis that can draw on all relevant sources of information. The biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information.

The U.S. government has access to a vast amount of information. When databases not usually thought of as "intelligence," such as customs or immigration information, are included, the storehouse is immense. But the U.S. government has a weak system for processing and using what it has. In interviews around the government, official after official urged us to call attention to frustrations with the unglamorous "back office" side of government operations.

In the 9/11 story, for example, we sometimes see examples of information that could be accessed—like the undistributed NSA information that would have helped identify Nawaf al Hazmi in January 2000. But someone had to ask for it. In that case, no one did. Or, as in the episodes we describe in chapter 8, the information is distributed, but in a compartmented channel. Or the information is available, and someone does ask, but it cannot be shared.

What all these stories have in common is a system that requires a demonstrated "need to know" before sharing. This approach assumes it is possible to know, in advance, who will need to use the information. Such a system implicitly assumes that the risk of inadvertent disclosure outweighs the benefits of wider sharing. Those Cold War assumptions are no longer appropriate. The culture of agencies feeling they own the information they gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty to the information—to repay the taxpayers' investment by making that information available.

Each intelligence agency has its own security practices, outgrowths of the Cold War. We certainly understand the reason for these practices. Counterintelligence concerns are still real, even if the old Soviet enemy has been replaced by other spies.

But the security concerns need to be weighed against the costs. Current security requirements nurture overclassification and excessive compartmentation of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though these costs—even in literal financial terms—are substantial. There are no punishments for *not* sharing information. Agencies uphold a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration.[15]

Recommendation: Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge.

Intelligence gathered about transnational terrorism should be processed, turned into reports, and distributed according to the same quality standards, whether it is collected in Pakistan or in Texas.

The logical objection is that sources and methods may vary greatly in different locations. We therefore propose that when a report is first created, its data be separated from the sources and methods by which they are obtained. The report should begin with the information in its most shareable, but still meaningful, form. Therefore the maximum number of recipients can access some form of that information. If knowledge of further details becomes important, any user can query further, with access granted or denied according to the rules set for the network—and with queries leaving an audit trail in order to determine who accessed the information. But the questions may not come at all unless experts at the "edge" of the network can readily discover the clues that prompt to them.[16]

We propose that information be shared horizontally, across new networks that transcend individual agencies.

- The current system is structured on an old mainframe, or hub-and-spoke, concept. In this older approach, each agency has its own database. Agency users send information to the database and then can retrieve it from the database.
- A decentralized network model, the concept behind much of the information revolution, shares data horizontally too. Agencies would still have their own databases, but those databases would be searchable across agency lines. In this system, secrets are protected through the design of the network and an "information rights management" approach that controls access to the data, not access to the whole network. An outstanding conceptual framework for this kind of "trusted information network" has been developed by a task force of leading professionals in national security, information technology, and law assembled by the Markle Foundation. Its report has been widely discussed throughout the U.S. government, but has not yet been converted into action.[17]

Recommendation: The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should

coordinate the resolution of the legal, policy, and technical issues across agencies to create a "trusted information network."

- No one agency can do it alone. Well-meaning agency officials are under tremendous pressure to update their systems. Alone, they may only be able to modernize the stovepipes, not replace them.
- Only presidential leadership can develop government-wide concepts and standards. Currently, no one is doing this job. Backed by the Office of Management and Budget, a new National Intelligence Director empowered to set common standards for information use throughout the community, and a secretary of homeland security who helps extend the system to public agencies and relevant private-sector databases, a government-wide initiative can succeed.
- White House leadership is also needed because the policy and legal issues are harder than the technical ones. The necessary technology already exists. What does not are the rules for acquiring, accessing, sharing, and using the vast stores of public and private data that may be available. When information sharing works, it is a powerful tool. Therefore the sharing and uses of information must be guided by a set of practical policy guidelines that simultaneously empower and constrain officials, telling them clearly what is and is not permitted.

"This is government acting in new ways, to face new threats," the most recent Markle report explains. "And while such change is necessary, it must be accomplished while engendering the people's trust that privacy and other civil liberties are being protected, that businesses are not being unduly burdened with requests for extraneous or useless information, that taxpayer money is being well spent, and that, ultimately, the network will be effective in protecting our security." The authors add: "Leadership is emerging from all levels of government and from many places in the private sector. What is needed now is a plan to accelerate these efforts, and public debate and consensus on the goals."[18] . . .

13.5 ORGANIZING AMERICA'S DEFENSES IN THE UNITED STATES

The Future Role of the FBI

We have considered proposals for a new agency dedicated to intelligence collection in the United States. Some call this a proposal for an "American MI-5," although the analogy is weak—the actual British Security Service is a relatively small worldwide agency that combines duties assigned in the U.S. government to the Terrorist Threat Integration Center, the CIA, the FBI, and the Department of Homeland Security.

The concern about the FBI is that it has long favored its criminal justice mission over its national security mission. Part of the reason for this is the demand around the country for FBI help on criminal matters. The FBI was criticized, rightly, for the overzealous domestic intelligence investigations disclosed during the 1970s. The pendulum swung away from those types of investigations during the 1980s and 1990s, though the FBI maintained an active counterintelligence function and was the lead agency for the investigation of foreign terrorist groups operating inside the United States.

We do not recommend the creation of a new domestic intelligence agency. It is not needed if our other recommendations are adopted—to establish a strong national

intelligence center, part of the NCTC, that will oversee counterterrorism intelligence work, foreign and domestic, and to create a National Intelligence Director who can set and enforce standards for the collection, processing, and reporting of information.

Under the structures we recommend, the FBI's role is focused, but still vital. The FBI does need to be able to direct its thousands of agents and other employees to collect intelligence in America's cities and towns—interviewing informants, conducting surveillance and searches, tracking individuals, working collaboratively with local authorities, and doing so with meticulous attention to detail and compliance with the law. The FBI's job in the streets of the United States would thus be a domestic equivalent, operating under the U.S. Constitution and quite different laws and rules, to the job of the CIA's operations officers abroad.

Creating a new domestic intelligence agency has other drawbacks.

- The FBI is accustomed to carrying out sensitive intelligence collection operations in compliance with the law. If a new domestic intelligence agency were outside of the Department of Justice, the process of legal oversight—never easy—could become even more difficult. Abuses of civil liberties could create a backlash that would impair the collection of needed intelligence.
- Creating a new domestic intelligence agency would divert attention of the officials most responsible for current counterterrorism efforts while the threat remains high. Putting a new player into the mix of federal agencies with counterterrorism responsibilities would exacerbate existing information-sharing problems.
- A new domestic intelligence agency would need to acquire assets and personnel. The FBI already has 28,000 employees; 56 field offices, 400 satellite offices, and 47 legal attaché offices; a laboratory, operations center, and training facility; an existing network of informants, cooperating defendants, and other sources; and relationships with state and local law enforcement, the CIA, and foreign intelligence and law enforcement agencies.
- Counterterrorism investigations in the United States very quickly become matters that involve violations of criminal law and possible law enforcement action. Because the FBI can have agents working criminal matters and agents working intelligence investigations concerning the same international terrorism target, the full range of investigative tools against a suspected terrorist can be considered within one agency. The removal of "the wall" that existed before 9/11 between intelligence and law enforcement has opened up new opportunities for cooperative action within the FBI.
- Counterterrorism investigations often overlap or are cued by other criminal investigations, such as money laundering or the smuggling of contraband. In the field, the close connection to criminal work has many benefits.

Our recommendation to leave counterterrorism intelligence collection in the United States with the FBI still depends on an assessment that the FBI—if it makes an all-out effort to institutionalize change—can do the job. As we mentioned in chapter 3, we have been impressed by the determination that agents display in tracking down details, patiently going the extra mile and working the extra month, to put facts in the place of speculation. In our report we have shown how agents in Phoenix, Minneapolis, and New York displayed initiative in pressing their investigations.

FBI agents and analysts in the field need to have sustained support and dedicated resources to become stronger intelligence officers. They need to be rewarded for acquiring informants and for gathering and disseminating information differently and more broadly than usual in a traditional criminal investigation. FBI employees need to report and analyze what they have learned in ways the Bureau has never done before.

Under Director Robert Mueller, the Bureau has made significant progress in improving its intelligence capabilities. It now has an Office of Intelligence, overseen by the top tier of FBI management. Field intelligence groups have been created in all field offices to put FBI priorities and the emphasis on intelligence into practice. Advances have been made in improving the Bureau's information technology systems and in increasing connectivity and information sharing with intelligence community agencies.

Director Mueller has also recognized that the FBI's reforms are far from complete. He has outlined a number of areas where added measures may be necessary. Specifically, he has recognized that the FBI needs to recruit from a broader pool of candidates, that agents and analysts working on national security matters require specialized training, and that agents should specialize within programs after obtaining a generalist foundation. The FBI is developing career tracks for agents to specialize in counterterrorism/counterintelligence, cyber crimes, criminal investigations, or intelligence. It is establishing a program for certifying agents as intelligence officers, a certification that will be a prerequisite for promotion to the senior ranks of the Bureau. New training programs have been instituted for intelligence-related subjects.

The Director of the FBI has proposed creating an Intelligence Directorate as a further refinement of the FBI intelligence program. This directorate would include units for intelligence planning and policy and for the direction of analysts and linguists.

We want to ensure that the Bureau's shift to a preventive counterterrorism posture is more fully institutionalized so that it survives beyond Director Mueller's tenure. We have found that in the past the Bureau has announced its willingness to reform and restructure itself to address transnational security threats, but has fallen short—failing to effect the necessary institutional and cultural changes organization-wide. We want to ensure that this does not happen again. Despite having found acceptance of the Director's clear message that counterterrorism is now the FBI's top priority, two years after 9/11 we also found gaps between some of the announced reforms and the reality in the field. We are concerned that management in the field offices still can allocate people and resources to local concerns that diverge from the national security mission. This system could revert to a focus on lower-priority criminal justice cases over national security requirements.

Recommendation: A specialized and integrated national security workforce should be established at the FBI consisting of agents, analysts, linguists, and surveillance specialists who are recruited, trained, rewarded, and retained to ensure the development of an institutional culture imbued with a deep expertise in intelligence and national security.

- The president, by executive order or directive, should direct the FBI to develop this intelligence cadre.
- Recognizing that cross-fertilization between the criminal justice and national security disciplines is vital to the success of both missions, all new agents should receive basic training in both areas. Furthermore, new agents should begin their careers with meaningful assignments in both areas.

- Agents and analysts should then specialize in one of these disciplines and have the option to work such matters for their entire career with the Bureau. Certain advanced training courses and assignments to other intelligence agencies should be required to advance within the national security discipline.
- In the interest of cross-fertilization, all senior FBI managers, including those working on law enforcement matters, should be certified intelligence officers.
- The FBI should fully implement a recruiting, hiring, and selection process for agents and analysts that enhances its ability to target and attract individuals with educational and professional backgrounds in intelligence, international relations, language, technology, and other relevant skills.
- The FBI should institute the integration of analysts, agents, linguists, and surveillance personnel in the field so that a dedicated team approach is brought to bear on national security intelligence operations.
- Each field office should have an official at the field office's deputy level for national security matters. This individual would have management oversight and ensure that the national priorities are carried out in the field.
- The FBI should align its budget structure according to its four main programs—intelligence, counterterrorism and counterintelligence, criminal, and criminal justice services—to ensure better transparency on program costs, management of resources, and protection of the intelligence program.[19]
- The FBI should report regularly to Congress in its semiannual program reviews designed to identify whether each field office is appropriately addressing FBI and national program priorities.
- The FBI should report regularly to Congress in detail on the qualifications, status, and roles of analysts in the field and at headquarters. Congress should ensure that analysts are afforded training and career opportunities on a par with those offered analysts in other intelligence community agencies.
- The Congress should make sure funding is available to accelerate the expansion of secure facilities in FBI field offices so as to increase their ability to use secure email systems and classified intelligence product exchanges. The Congress should monitor whether the FBI's information-sharing principles are implemented in practice.

The FBI is just a small fraction of the national law enforcement community in the United States, a community comprised mainly of state and local agencies. The network designed for sharing information, and the work of the FBI through local joint Terrorism Task Forces, should build a reciprocal relationship, in which state and local agents understand what information they are looking for and, in return, receive some of the information being developed about what is happening, or may happen, in their communities. In this relationship, the Department of Homeland Security also will play an important part.

The Homeland Security Act of 2002 gave the under secretary for information analysis and infrastructure protection broad responsibilities. In practice, this directorate has the job to map "terrorist threats to the homeland against our assessed vulnerabilities in order to drive our efforts to protect against terrorist threats."[20] These capabilities are still embryonic. The directorate has not yet developed the capacity to perform one of its assigned jobs, which is to assimilate and analyze information from Homeland Security's own component agencies, such as the Coast Guard, Secret Service, Transportation Security Administration, Immigration and Customs Enforcement, and Customs and Border

Protection. The secretary of homeland security must ensure that these components work with the Information Analysis and Infrastructure Protection Directorate so that this office can perform its mission.[21]

Homeland Defense

At several points in our inquiry, we asked, "Who is responsible for defending us at home?" Our national defense at home is the responsibility, first, of the Department of Defense and, second, of the Department of Homeland Security. They must have clear delineations of responsibility and authority.

We found that NORAD, which had been given the responsibility for defending U.S. airspace, had construed that mission to focus on threats coming from outside America's borders. It did not adjust its focus even though the intelligence community had gathered intelligence on the possibility that terrorists might turn to hijacking and even use of planes as missiles. We have been assured that NORAD has now embraced the full mission. Northern Command has been established to assume responsibility for the defense of the domestic United States.

Recommendation: The Department of Defense and its oversight committees should regularly assess the adequacy of Northern Command's strategies and planning to defend the United States against military threats to the homeland.

The Department of Homeland Security was established to consolidate all of the domestic agencies responsible for securing America's borders and national infrastructure, most of which is in private hands. It should identify those elements of our transportation, energy, communications, financial, and other institutions that need to be protected, develop plans to protect that infrastructure, and exercise the mechanisms to enhance preparedness. This means going well beyond the preexisting jobs of the agencies that have been brought together inside the department.

Recommendation: The Department of Homeland Security and its oversight committees should regularly assess the types of threats the country faces to determine (a) the adequacy of the government's plans—and the progress against those plans—to protect America's critical infrastructure and (b) the readiness of the government to respond to the threats that the United States might face.

• • •

We look forward to a national debate on the merits of what we have recommended, and we will participate vigorously in that debate.

NOTES

1. The Bush administration clarified the respective missions of the different intelligence analysis centers in a letter sent by Secretary ridge, DCI Tenet, FBI Director Mueller, and TTIC Director Brennan to Senators Susan Collins and Carl Levin on April 13, 2004. The letter did not mention any element of the Department of Defense. It stated that the DCI would define what analytical resources he would transfer from the CTC to TTIC no later than June 1, 2004. DCI Tenet

subsequently told us that he decided that TTIC would have primary responsibility for terrorism analysis but that the CIA and the Defense Intelligence Agency would grow their own analysts. TTIC will have tasking authority over terrorism analysts in other intelligence agencies, although there will need to be a board to supervise deconfliction. George Tenet interview (July 2, 2004). We have not received any details regarding this plan.

2. "TTIC has no operational authority. However, TTIC has the authority to task collection and analysis from Intelligence Community agencies, the FBI, and DHS through tasking mechanisms we will create. The analytic work conducted at TTIC creates products that inform each of TTIC's partner elements, as well as other Federal departments and agencies as appropriate." Letter from Ridge and others to Collins and Levin, Apr. 13, 2004.

3. Donald Rumsfeld prepared statement, Mar. 23, 2004, p. 20.

4. In this conception, the NCTC should plan actions, assigning responsibilities for operational direction and execution to other agencies. It would be built on TTIC and would be supported by the intelligence community as TTIC is now. Whichever route is chosen, the scarce analytical resources now dispersed among TTIC, the Defense Intelligence Agency's Joint Interagency Task Force—Combatting Terrorism (JITF-CT), and the DCI's Counterterrorist Center (CTC) should be concentrated more effectively than they are now.

- The DCI's Counterterrorist Center would become a CIA unit, to handle the direction and execution of tasks assigned to the CIA. It could have detailees from other agencies, as it does now, to perform this operational mission. It would yield much of the broader, strategic analytic duties and personnel to the NCTC. The CTC would rely on the restructured CIA (discussed in section 13.2) to organize, train, and equip its personnel.
- Similarly, the FBI's Counterterrorism Division would remain, as now, the operational arm of the Bureau to combat terrorism. As it does now, it would work with other agencies in carrying out these missions, retaining the JTTF structure now in place. The Counterterrorism Division would rely on the FBI's Office of Intelligence to train and equip its personnel, helping to process and report the information gathered in the field.
- The Defense Department's unified commands—SOCOM, NORTHCOM, and CENTCOM—would be the joint operational centers taking on DOD tasks. Much of the excellent analytical talent that has been assembled in the Defense Intelligence Agency's JITF-CT should merge into the planned NCTC.
- The Department of Homeland Security's Directorate for Information Analysis and Infrastructure Protection should retain its core duties, but the NCTC should have the ultimate responsibility for producing *net* assessments that utilize Homeland Security's analysis of domestic vulnerabilities and integrate all-source analysis of foreign intelligence about the terrorist enemy.
- The State Department's counterterrorism office would be a critical participant in the NCTC's work, taking the lead in directing the execution of the counterterrorism foreign policy mission.

The proposed National Counterterrorism Center should offer one-stop shopping to agencies with counterterrorism and homeland security responsibilities. That is, it should be an authoritative reference base on the transnational terrorist organizations: their people, goals, strategies, capabilities, networks of contacts and support, the context in which they operate, and their characteristic habits across the life cycle of operations—recruitment, reconnaissance, target selection, logistics, and travel. For example, this Center would offer an integrated depiction of groups like al Qaeda or Hezbollah worldwide, overseas, and in the United States.

The NCTC will not eliminate the need for the executive departments to have their own analytic units. But it would enable agency-based analytic units to become smaller and more efficient. In particular, it would make it possible for these agency-based analytic units to concentrate on analysis that is tailored to their agency's specific responsibilities.

A useful analogy is in military intelligence. There, the Defense Intelligence Agency and the service production agencies (like the Army's National Ground Intelligence Center) are the institutional memory and reference source for enemy order of battle, enemy organization, and enemy equipment. Yet the Joint Staff and all the theater commands still have their own J-2s. They draw on the information they need, tailoring and applying it to their operational needs. As they learn more from their tactical operations, they pass intelligence of enduring value back up to the Defense Intelligence Agency and the services so it can be evaluated, form part of the institutional memory, and help guide future collection.

In our proposal, that reservoir of institutional memory about terrorist organizations would function for the government as a whole, and would be in the NCTC.

5. The head of the NCTC would thus help coordinate the operational side of these agencies, like the FBI's Counterterrorism Division. The intelligence side of these agencies, such as the FBI's Office of Intelligence, would be overseen by the National Intelligence Director we recommend later in this chapter.

6. The quotation goes on: "It includes gaps in intelligence, but also intelligence that, like a string of pearls too precious to wear, is too sensitive to give to those who need it. It includes the alarm that fails to work, but also the alarm that has gone off so often it has been disconnected. It includes the unalert watchman, but also the one who knows he'll be chewed out by his superior if he gets higher authority out of bed. It includes the contingencies that occur to no one, but also those that everyone assumes somebody else is taking care of. It includes straightforward procrastination, but also decisions protracted by internal disagreement. It includes, in addition, the inability of individual human beings to rise to the occasion until they are sure it is the occasion—which is usually too late. . . . Finally, as at Pearl Harbor, surprise may include some measure of genuine novelty introduced by the enemy, and some sheer bad luck." Thomas Schelling, foreword to Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford Univ. Press, 1962), p. viii.

7. For the Goldwater-Nichols Act, see Pub. L. No. 99–433, 100 Stat. 992 (1986). For a general discussion of the act, see Gordon Lederman, *Reorganizing the Joint Chiefs of Staff: The Goldwater-Nichols Act of 1986* (Greenwood, 1999); James Locher, *Victory on the Potomac: The Goldwater-Nichols Act Unifies the Pentagon* (Texas A&M Univ. Press, 2003).

8. For a history of the DCI's authority over the intelligence community, see CIA report, Michael Warner ed., *Central Intelligence; Origin and Evolution* (CIA Center for the Study of Intelligence, 2001). For the Director's view of his community authorities, see DCI directive, "Director of Central Intelligence Directive 1/1: The Authorities and Responsibilities of the Director of Central Intelligence as Head of the U.S. Intelligence Community," Nov. 19, 1998.

9. As Norman Augustine, former chairman of Lockheed Martin Corporation, writes regarding power in the government, "As in business, cash is king. If you are not in charge of your budget, you are not king." Norman Augustine, *Managing to Survive in Washington: A Beginner's Guide to High-Level Management in Government* (Center for Strategic and International Studies, 2000), p. 20.

10. For the DCI and the secretary of defense, see 50 U.S.C. § 403-6(a). If the director does not concur with the secretary's choice, then the secretary is required to notify the president of the director's nonconcurrence. Ibid. For the DCI and the attorney general, see 50 U.S.C. § 403-6(b)(3).

11. The new program would replace the existing National Foreign Intelligence Program.

12. Some smaller parts of the current intelligence community, such as the State Department's intelligence bureau and the Energy Department's intelligence entity, should not be funded out of the national intelligence program and should be the responsibility of their home departments.

13. The head of the NCTC should have the rank of a deputy national intelligence director, e.g., Executive Level II, but would have a different title.

14. If the organization of defense intelligence remains as it is now, the appropriate official would be the under secretary of defense for intelligence. If defense intelligence is reorganized to elevate the responsibilities of the director of the DIA, then that person might be the appropriate official.

15. For the information technology architecture, see Ruth David interview (June 10, 2003). For the necessity of moving from need-to-know to need-to-share, see James Steinberg testimony, Oct. 14,

2003. The Director still has to strategy for removing information-sharing barriers and—more than two years since 9/11—has only appointed a working group on the subject. George Tenet prepared statement, Mar. 24, 2004, p. 37.

16. The intelligence community currently makes information shareable by creating "tearline" reports, with the nonshareable information at the top and then, below the "tearline," the portion that recipients are told they can share. This proposal reverses that concept. All reports are created as tearline data, with the shareable information at the top and with added details accessible on a system that requires permissions or authentication.

17. See Markle Foundation Task Force report, *Creating a Trusted Information Network for Homeland Security* (Markle Foundation, 2003); Markle Foundation Task Force report, *Protecting America's Freedom in the Information Age* (Markle Foundation, 2002) (both online at www.markle.org).

18. Markle Foundation Task Force report, *Creating a Trusted Information Network*, p. 12. The pressing need for such guidelines was also spotlighted by the Technology and Privacy Advisory Committee appointed by Secretary Rumsfeld to advise the Department of Defense on the privacy implications of its Terrorism Information Awareness Program. Technology and Privacy Advisory Committee report, *Safeguarding Privacy in the Fight Against Terrorism* (2004) (online at www.sainc.com/tapac/TAPAC_Report_Final_5-10-04.pdf). We take no position on the particular recommendations offered in that report, but it raises issues that pertain to the government as a whole—not just to the Department of Defense.

19. This recommendation, and measures to assist the Bureau in developing its intelligence cadre, are included in the report accompanying the Commerce, Justice and State Appropriations Act for Fiscal Year 2005, passed by the House of Representatives on July 7, 2004. H.R. Rep. No. 108–576, 108th Cong., 2d sess. (2004), p. 22.

20. Letter from Ridge and others to Collins and Levin, Apr. 13, 2004.

21. For the directorate's current capability, see Patrick Hughes interview (Apr. 2, 2004).

APPENDIX F

THE SILBERMAN-ROBB COMMISSION RECOMMENDATIONS ON INTELLIGENCE AND WMDS IN IRAQ, 2005

Editor's Note: The Department of Defense Commission investigating the incorrect intelligence assessments about weapons of mass destruction in Iraq reported on its findings in 2005. Led by Judge Laurence Silberman and former Senator Chuck Robb (D-VA), the Silberman-Robb Commission offered a number of recommendations on how intelligence might be improved to avoid similar mistakes in the future with regard to WMDs and terrorist activities. This appendix summarizes the panel's key findings.

COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION WASHINGTON, D.C. 20503

CO-CHAIRMEN:

THE HONORABLE
LAURENCE H. SILBERMAN

THE HONORABLE
CHARLES S. ROBB

March 31, 2005

Mr. President:

With this letter, we transmit the report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Our unanimous report is based on a lengthy investigation, during which we interviewed hundreds of experts from inside and outside the Intelligence Community and reviewed thousands of documents. Our report offers 74 recommendations for improving the U.S. Intelligence Community (all

Source: The Silberman-Robb Commission, Washington, DC, 2005, pp. 399–428.

but a handful of which we believe can be implemented without statutory change). But among these recommendations a few points merit special emphasis.

We conclude that the Intelligence Community was dead wrong in almost all of its pre-war judgments about Iraq's weapons of mass destruction. This was a major intelligence failure. Its principal causes were the Intelligence Community's inability to collect good information about Iraq's WMD programs, serious errors in analyzing what information it could gather, and a failure to make clear just how much of its analysis was based on assumptions, rather than good evidence. On a matter off this importance, we simply cannot afford failures of this magnitude.

After a thorough review, the Commission found no indication that the Intelligence Community distorted the evidence regarding Iraq's weapons of mass destruction. What the intelligence professionals told you about Saddam Hussein's programs was what they believed. They were simply wrong.

As you asked, we looked as well beyond Iraq in our review of the Intelligence Community's capabilities. We conducted case studies of our intelligence agencies' recent performance assessing the risk of WMD in Libya and Afghanistan, and our current capabilities with respect to several of the world's most dangerous state and non-state proliferation threats. Out of this more comprehensive review, we report both bad news and good news. The bad news is that we still know disturbingly little about the weapons programs and even less about the intentions of many of our most dangerous adversaries. The good news is that we have had some solid intelligence successes—thanks largely to innovative and multi-agency collection techniques.

Our review has convinced us that the best hope for preventing future failures is dramatic change. We need an Intelligence Community that is truly integrated, far more imaginative and willing to run risks, open to a new generation of Americans, and receptive to new technologies.

We have summarized our principal recommendations for the entire Intelligence Community in the Overview of the report. Here, we focus on recommendations that we believe only you can effect if you choose to implement them:

- ***Give the DNI powers—and backing—to match his responsibilities.***

In your public statement accompanying the announcement of Ambassador Negroponte's nomination as Director of National Intelligence (DNI), you have already moved in this direction. The new intelligence law makes the DNI responsible for integrating the 15 independent members of the Intelligence Community. But it gives him powers that are only relatively broader than before. The DNI cannot make this work unless he takes his legal authorities over the budget, programs, personnel, and priorities to the limit. It won't be easy to provide this leadership to the intelligence components of the Defense Department, or to the CIA. They are some of the government's most headstrong agencies. Sooner or later, they will try to run around—or over—the DNI. Then, only your determined backing will convince them that we cannot return to the old ways.

- ***Bring the FBI all the way into the Intelligence Community.***

The FBI is one of the proudest and most independent agencies in the United States Government. It is on its way to becoming an effective intelligence agency, but it will never

arrive if it insists on using only is own map. We recommend that you order an organizational reform of the Bureau that pulls all of its intelligence capabilities into one place and subjects them to the coordinating authority of the DNI—the same authority that the DNI exercises over Defense Department intelligence agencies. Under this recommendation, the counterterrorism and counterintelligence resources of the Bureau would become a single National Security Service inside the FBI. It would of course still be subject to the Attorney General's oversight and to current legal rules. The intelligence reform act almost accomplishes this task, but at crucial points it retreats into ambiguity. Without leadership from the DNI, the FBI is likely to continue escaping effective integration into the Intelligence Community.

- ***Demand more of the Intelligence Community.***

The Intelligence Community needs to be pushed. It will not do its best unless it is pressed by polilcymakers—sometimes to the point of discomfort. Analysts must be pressed to explain how much they don't know; the collection agencies must be pressed to explain why they don't have better information on key topics. While policyinakers must be prepared to credit ntelligence that doesn't fit their preferences, no important intelligence assessment should be accepted without sharp questioning that forces the community to explain exactly how it came to that assessment and what alternatives might also be true. This is not "politicization"; it is a necessary part of the intelligence process. And in the end, it is the key to getting the best from an Intelligence Community that, at its best, knows how to do astonishing things.

- ***Rethink the President's Daily Brief.***

The daily intelligence briefings given to you before the Iraq war were flawed. Through attention-grabbing headlines and repetition of questionable data, these briefings overstated the case that Iraq was rebuilding its WMD programs. There are many other aspects of the daily brief that deserve to be reconsidered as well, but we are reluctant to make categorical recommendations on a process that in the end must meet your needs, not our theories. On one point, however, we want to be specific: while the DNI must be ultimately responsible for the content of your daily briefing, we do not believe that the DNI ought to prepare, deliver, or even attend every briefing. For if the DNI is consumed by current intelligence, the long-term needs of the Intelligence Community will suffer.

* * *

There is no more important intelligence mission important intelligence than understanding the worst weapons that our enemies possess, and how they intend to use them against us. These are their deepest secrets, and unlocking them must be our highest priority. So far, despite some successes, our Intelligence Community has not been agile and innovative enough to provide the information that the nation needs. Other commissions and observers have said the same. We should not wait for another

commission or another Administration to force widespread change in the Intelligence Community.

Very respectfully,

Laurence H. Silberman
Co-Chairman

Charles S. Robb
Co-Chairman

Richard C. Levin John McCain Henry S. Rowen Walter B. Slocombe
William O. Studeman Patricia M. Wald Charles M. Vest

Lloyd Cutler
(Of Counsel)

OVERVIEW OF THE REPORT

INTRODUCTION

On the brink of war, and in front of the whole world, the United States government asserted that Saddam Hussein had reconstituted his nuclear weapons program, had biological weapons and mobile biological weapon production facilities, and had stockpiled and was producing chemical weapons. All of this was based on the assessments of the U.S. Intelligence Community. And not one bit of it could be confirmed when the war was over.

While the intelligence services of many other nations also thought that Iraq had weapons of mass destruction, in the end it was the United States that put its credibility on the line, making this one of the most public—and most damaging—intelligence failures in recent American history.

This failure was in large part the result of analytical shortcomings; intelligence analysts were too wedded to their assumptions about Saddam's intentions. But it was also a failure on the part of those who collect intelligence—CIA's and the Defense Intelligence Agency's (DIA) spies, the National Security Agency's (NSA) eavesdroppers, and the National Geospatial-Intelligence Agency's (NGA) imagery experts.[1] In the end, those agencies collected precious little intelligence for the analysts to analyze, and much of what they did collect was either worthless or misleading. Finally, it was a failure to communicate effectively with policymakers; the Intelligence Community didn't adequately explain just how little good intelligence it had—or how much its assessments were driven by assumptions and inferences rather than concrete evidence.

Was the failure in Iraq typical of the Community's performance? Or was Iraq, as one senior intelligence official told the Commission, a sort of "perfect storm"—a one-time breakdown caused by a rare confluence of events that conspired to create a bad result? In our view, it was neither.

The failures we found in Iraq are not repeated everywhere. The Intelligence Community played a key role, for example, in getting Libya to renounce weapons of mass destruction and in exposing the long-running A.Q. Khan nuclear proliferation network. It is engaged in imaginative, successful (and highly classified) operations in many parts of the world. Tactical support to counterterrorism efforts is excellent, and there are signs of a boldness that would have been unimaginable before September 11, 2001.

But neither was Iraq a "perfect storm." The flaws we found in the Intelligence Community's Iraq performance are still all too common. Across the board, the Intelligence Community knows disturbingly little about the nuclear programs of many of the world's most dangerous actors. In some cases, it knows less now than it did five or ten years ago. As for biological weapons, despite years of Presidential concern, the Intelligence Community has struggled to address this threat.

To be sure, the Intelligence Community is full of talented, dedicated people. But they seem to be working harder and harder just to maintain a *status quo* that is increasingly irrelevant to the new challenges presented by weapons of mass destruction. Our collection agencies are often unable to gather intelligence on the very things we care the most about.

---

[1] While we have attempted to write this report in a way that is accessible to those not acquainted with the world of intelligence, we have included a primer on the U.S. Intelligence Community at Appendix C of this report for readers who are new to the subject.

Too often, analysts simply accept these gaps; they do little to help collectors identify new opportunities, and they do not always tell decisionmakers just how limited their knowledge really is.

Taken together, these shortcomings reflect the Intelligence Community's struggle to confront an environment that has changed radically over the past decade. For almost 50 years after the passage of the National Security Act of 1947, the Intelligence Community's resources were overwhelmingly trained on a single threat—the Soviet Union, its nuclear arsenal, its massive conventional forces, and its activities around the world. By comparison, today's priority intelligence targets are greater in number (there are dozens of entities that could strike a devastating blow against the United States) and are often more diffuse in character (they include not only states but also nebulous transnational terror and proliferation networks). What's more, some of the weapons that would be most dangerous in the hands of terrorists or rogue nations are difficult to detect. Much of the technology, equipment, and materials necessary to develop biological and chemical weapons, for example, also has legitimate commercial applications. Biological weapons themselves can be built in small-scale facilities that are easy to conceal, and weapons-grade uranium can be effectively shielded from traditional detection techniques. At the same time, advances in technology have made the job of technical intelligence collection exceedingly difficult.

The demands of this new environment can only be met by broad and deep change in the Intelligence Community. The Intelligence Community we have today is buried beneath an avalanche of demands for "current intelligence"—the pressing need to meet the tactical requirements of the day. Current intelligence in support of military and other action is necessary, of course. But we also need an Intelligence Community with *strategic* capabilities: it must be equipped to develop long-term plans for penetrating today's difficult targets, and to identify political and social trends shaping the threats that lie over the horizon. We can imagine no threat that demands greater strategic focus from the Intelligence Community than that posed by nuclear, biological, and chemical weapons.

The Intelligence Community is also fragmented, loosely managed, and poorly coordinated; the 15 intelligence organizations are a "Community" in name only and rarely act with a unity of purpose. What we need is an Intelligence Community that is *integrated*: the Community's leadership must be capable of allocating and directing the Community's resources in a coordinated way. The strengths of our distinct collection agencies must be brought to bear together on the most difficult intelligence problems. At the same time we need a Community that preserves diversity of analysis, and that encourages structured debate among agencies and analysts over the interpretation of information.

Perhaps above all, the Intelligence Community is too slow to change the way it does business. It is reluctant to use new human and technical collection methods; it is behind the curve in applying cutting-edge technologies; and it has not adapted its personnel practices and incentives structures to fit the needs of a new job market. What we need is an Intelligence Community that is flexible—able to respond nimbly to an ever-shifting threat environment and to the rapid pace of today's technological changes.

In short, to succeed in confronting today's and tomorrow's threats, the Intelligence Community must be transformed—a goal that would be difficult to meet even in the best of all possible worlds. And we do not live in the best of worlds. The CIA and NSA may be sleek and omniscient in the movies, but in real life they and other intelligence agencies are vast government bureaucracies. They are bureaucracies filled with talented people and armed with sophisticated technological tools, but talent and tools do not suspend the iron

laws of bureaucratic behavior. Like government bodies everywhere, intelligence agencies are prone to develop self-reinforcing, risk averse cultures that take outside advice badly. While laudable steps were taken to improve our intelligence agencies after September 11, 2001, the agencies have done less in response to the failures over Iraq, and we believe that many within those agencies do not accept the conclusion that we reached after our year of study: that the Community needs fundamental change if it is to successfully confront the threats of the 21st century.

We are not the first to say this. Indeed, commission after commission has identified some of the same fundamental failings we see in the Intelligence Community, usually to little effect. The Intelligence Community is a closed world, and many insiders admitted to us that *it has an almost perfect record of resisting external recommendations.*

But the present moment offers an unprecedented opportunity to overcome this resistance. About halfway through our inquiry, Congress passed the *Intelligence Reform and Terrorism Prevention Act of 2004*, which became a sort of a *dens ex machina* in our deliberations. The act created a Director of National Intelligence (DNI). The DNI's role could have been a purely coordinating position, with a limited staff and authority to match. Or it could have been something closer to a "Secretary of Intelligence," with full authority over the principal intelligence agencies and clear responsibility for their actions—which also might well have been consistent with a small bureaucratic superstructure. In the end, the DNI created by the intelligence reform legislation was neither of these things; the office is given broad responsibilities but only ambiguous authorities. While we might have chosen a different solution, we are not writing on a blank slate. So our focus has been in large part on how to make the new intelligence structure work, and in particular on giving the DNI tools (and support staff) to match his large responsibilities.

We are mindful, however, that there is a serious risk in creating too large a bureaucratic structure to serve the DNI: the risk that decisionmaking in the field, which sometimes requires quick action, will be improperly delayed. Balancing these two imperatives—necessary agility of operational execution and thoughtful coordination of intelligence activities—is, in our view, the DNI's greatest challenge.

In considering organizational issues, we did not delude ourselves that organizational structure alone can solve problems. More than many parts of government, the culture of the Intelligence Community is formed in the field, where organizational changes at headquarters are felt only lightly. We understand the limits of organizational change, and many of our recommendations go beyond organizational issues and would, if enacted, directly affect the way that intelligence is collected and analyzed. But we regret that we were not able to make such detailed proposals for some of the most important technical collection agencies, such as NSA and NGA. For those agencies, and for the many other issues that we could only touch upon, we must trust that our broader institutional recommendations will enable necessary reform. The DNI that we envision will have the budget and management tools to dig deep into the culture of each agency and to force changes where needed.

This Overview—and, in far more detail, the report that follows—offers our conclusions on what needs to be done. We begin by describing the results of our case studies—which include Iraq, Libya, Afghanistan, and others—and the lessons they teach about the Intelligence Community's current capabilities and weaknesses. We then offer our recommendations for reform based upon those lessons.

Three final notes before proceeding. First, our main tasks were to find out how the Intelligence Community erred in Iraq and to recommend changes to avoid such errors in the

future. This is a task that often lends itself to hubris and to second-guessing, and we have been humbled by the difficult judgments that had to be made about Iraq and its weapons programs. We are humbled too by the complexity of the management and technical challenges intelligence professionals face today. We recommend substantial changes, and we believe deeply that such changes are necessary, but we recognize that other reasonable observers could come to a different view on some of these questions.

Second, no matter how much we improve the Intelligence Community, weapons of mass destruction will continue to pose an enormous threat. Intelligence will always be imperfect and, as history persuades us, surprise can never be completely prevented. Moreover, we cannot expect spies, satellites, and analysts to constitute our only defense. As our biological weapons recommendations make abundantly clear, all national capabilities—regulatory, military, and diplomatic—must be used to combat proliferation.

Finally, we emphasize two points about the scope of this Commission's charter, particularly with respect to the Iraq question. First, we were *not* asked to determine whether Saddam Hussein had weapons of mass destruction. That was the mandate of the Iraq Survey Group; our mission is to investigate the reasons why the Intelligence Community's pre-war assessments were so different from what the Iraq Survey Group found after the war. Second, we were not authorized to investigate how policymakers used the intelligence assessments they received from the Intelligence Community. Accordingly, while we interviewed a host of current and former policymakers during the course of our investigation, the purpose of those interviews was to learn about how the Intelligence Community reached and communicated its judgments about Iraq's weapons programs—not to review how policymakers subsequently used that information.

LOOKING BACK: CASE STUDIES IN FAILURE AND SUCCESS

Our first task was to evaluate the Intelligence Community's performance in assessing the nuclear, biological, and chemical weapons activities of three countries: Iraq, Afghanistan, and Libya. In addition, we studied U.S. capabilities against other pressing intelligence problems—including Iran, North Korea, Russia, China, and terrorism. We wanted a range of studies so we would not judge the Intelligence Community solely on its handling of Iraq, which was—however important—a single intelligence target. In all, the studies paint a representative picture. It is the picture of an Intelligence Community that urgently needs to be changed.

Iraq: An Overview

In October 2002, at the request of members of Congress, the National Intelligence Council produced a National Intelligence Estimate (NIE)—the most authoritative intelligence assessment produced by the Intelligence Community—which concluded that Iraq was reconstituting its nuclear weapons program and was actively pursuing a nuclear device. According to the exhaustive study of the Iraq Survey Group, this assessment was almost completely wrong. The NIE said that Iraq's biological weapons capability was larger and more advanced than before the Gulf War and that Iraq possessed mobile biological weapons production facilities. This was wrong. The NIE further stated that Iraq had renewed production of chemical weapons, including mustard, sarin, GF, and VX, and that it had accumulated chemical stockpiles of between 100 and 500 metric tons. All of this was

also wrong. Finally, the NIE concluded that Iraq had unmanned aerial vehicles that were probably intended for the delivery of biological weapons, and ballistic missiles that had ranges greater than the United Nations' permitted 150 kilometer range. In truth, the aerial vehicles were not for biological weapons; some of Iraq's missiles were, however, capable of traveling more than 150 kilometers. The Intelligence Community's Iraq assessments were, in short, riddled with errors.

Contrary to what some defenders of the Intelligence Community have since asserted, these errors were *not* the result of a few harried months in 2002. Most of the fundamental errors were made and communicated to policyrnakers well before the now-infamous NIE of October 2002, and were not corrected in the months between the NIE and the start of the war. They were not isolated or random failings. Iraq had been an intelligence challenge at the forefront of U.S. attention for over a decade. It was a known adversary that had already fought one war with the United States and seemed increasingly likely to fight another. But, after ten years of effort, the Intelligence Community still had no good intelligence on the status of Iraq's weapons programs. Our full report examines these issues in detail. Here we limit our discussion to the central lessons to be learned from this episode.

The first lesson is that the Intelligence Community cannot analyze and disseminate information that it does not have. The Community's Iraq assessment was crippled by its inability to collect meaningful intelligence on Iraq's nuclear, biological, and chemical weapons programs. The second lesson follows from the first: lacking good intelligence, analysts and collectors fell back on old assumptions and inferences drawn from Iraq's past behavior and intentions.

The Intelligence Community had learned a hard lesson after the 1991 Gulf War, which revealed that the Intelligence Community's pre-war assessments had underestimated Iraq's nuclear program and had failed to identify all of its chemical weapons storage sites. Shaken by the magnitude of their errors, intelligence analysts were determined not to fall victim again to the same mistake. This tendency was only reinforced by later events. Saddam acted to the very end like a man with much to hide. And the dangers of underestimating our enemies were deeply underscored by the attacks of September 11, 2001.

Throughout the 1990s, therefore, the Intelligence Community assumed that Saddam's Iraq was up to no good—that Baghdad had maintained its nuclear, biological, and chemical technical expertise, had kept its biological and chemical weapons production capabilities, and possessed significant stockpiles of chemical agents and weapons precursors. Since Iraq's leadership had not changed since 1991, the Intelligence Community also believed that these capabilities would be further revved up as soon as inspectors left Iraq. Saddam's continuing cat-and-mouse parrying with international inspectors only hardened these assumptions.

These experiences contributed decisively to the Intelligence Community's erroneous National Intelligence Estimate of October 2002. That is not to say that its fears and assumptions were foolish or even unreasonable. At some point, however, these premises stopped being working hypotheses and became more or less unrebuttable conclusions; worse, the intelligence system became too willing to find confirmations of them in evidence that should have been recognized at the time to be of dubious reliability. Collectors and analysts too readily accepted any evidence that supported their theory that Iraq had stockpiles and was developing weapons programs, and they explained away or simply disregarded evidence that pointed in the other direction.

Even in hindsight, those assumptions have a powerful air of common sense. If the Intelligence Community's estimate and other pre-war intelligence had relied principally

and explicitly on inferences the Community drew from Iraq's past conduct, the estimate would still have been wrong, but it would have been far more defensible. For good reason, it was hard to conclude that Saddam Hussein had indeed abandoned his weapons programs. But a central flaw of the NIE is that it took these defensible assumptions and swathed them in the mystique of intelligence, providing secret information that seemed to support them but was in fact nearly worthless, if not misleading. The NIE simply didn't communicate how weak the underlying intelligence was.

This was, moreover, a problem that was not limited to the NIE. Our review found that *after* the publication of the October 2002 NIE but *before* Secretary of State Colin Powell's February 2003 address to the United Nations, intelligence officials within the CIA failed to convey to policymakers new information casting serious doubt on the reliability of a human intelligence source known as "Curveball." This occurred despite the pivotal role Curveball's information played in the Intelligence Community's assessment of Iraq's biological weapons programs, and in spite of Secretary Powell's efforts to strip every dubious piece of information out of his proposed speech. In this instance, once again, the Intelligence Community failed to give policymakers a full understanding of the frailties of the intelligence on which they were relying.

Finally, we closely examined the possibility that intelligence analysts were pressured by policymakers to change their judgments about Iraq's nuclear, biological, and chemical weapons programs. The analysts who worked Iraqi weapons issues universally agreed that in no instance did political pressure cause them to skew or alter any of their analytical judgments. That said, it is hard to deny the conclusion that intelligence analysts worked in an environment that did not encourage skepticism about the conventional wisdom.

Other Case Studies: An Overview

Our remaining case studies present a more mixed picture. On the positive side, Libya is fundamentally a success story. The Intelligence Community assessed correctly the state of Libya's nuclear and chemical weapons programs, and the Intelligence Community's use of new techniques to penetrate the A.Q. Khan network allowed the U.S. government to pressure Libya into dismantling those programs. In counterterrorism, the Intelligence Community has made great strides since September 11, in particular with respect to tactical operations overseas. These successes stemmed from isolated efforts that need to be replicated in other areas of intelligence; in the case of Libya, from innovative collection techniques and, in the case of terrorism, from an impressive fusion of interagency intelligence capabilities.

But we also reviewed the state of the Intelligence Community's knowledge about the unconventional weapons programs of several countries that pose current proliferation threats, including Iran, North Korea, China, and Russia. We cannot discuss many of our findings from these studies in our unclassified report, but we can say here that we found that we have only limited access to critical information about several of these high-priority intelligence targets.

Lessons Learned from the Case Studies

Our case studies revealed failures and successes that ran the gamut of the intelligence process. Although each of these studies is covered in far greater detail in the report itself, we include here a summary of the central lessons we drew from them.

Poor target development: not getting intelligence on the issues we care about most. You can't analyze intelligence that you don't have—and our case studies resoundingly demonstrate how little we know about some of our highest priority intelligence targets. It is clear that in today's context the traditional collection techniques employed by individual collection agencies have lost much of their power to surprise our adversaries. The successful penetrations of "hard targets" that we did find were usually the result either of an innovative collection technique or of a creative integration of collection capabilities across agencies. In general, however, the Intelligence Community has not developed the long-term, coordinated collection strategies that are necessary to penetrate today's intelligence targets.

Lack of rigorous analysis. Long after the Community's assessment of Iraq had begun to fall apart, one of the main drafters of the NIE told us that, if he had to grade it, he would still give the NIE an "A." By that, he presumably meant that the NIE fully met the standards for analysis that the Community had set for itself. That is the problem. The scope and quality of analysis has eroded badly in the Intelligence Community and it must be restored. In part, this is a matter of tradecraft and training; in part, too, it is a matter of expertise.

Analytic "tradecraft"—the way analysts think, research, evaluate evidence, write, and communicate—must be strengthened. In many instances, we found finished intelligence that was loosely reasoned, ill-supported, and poorly communicated. Perhaps most worrisome, we found too many analytic products that obscured how little the Intelligence Community actually *knew* about an issue and how much their conclusions rested on inference and assumptions. We believe these tendencies must be reversed if decisionmakers are to have confidence in the intelligence they receive. And equally important, analysts must be willing to admit what they don't know in order to focus future collection efforts. Conversely, policymakers must be prepared to accept uncertainties and qualifications in intelligence judgments and not expect greater precision than the evaluated data permits.

Good "tradecraft" without expertise, however, will only get you so far. Our case studies identified areas in which the Community's level of expertise was far below what it should be. In several instances, the Iraq assessments rested on failures of technical analysis that should have been obvious at the time—failure to understand facts about weapons technology, for example, or failures to detect obvious forgeries. Technical expertise, particularly relating to weapons systems, has fallen sharply in the past ten years. And in other areas, such as biotechnology, the Intelligence Community is well behind the private sector.

But the problem of expertise goes well beyond technical knowledge. During the Cold War, the Intelligence Community built up an impressive body of expertise on Soviet society, organization, and ideology, as well as on the Soviet threat. Regrettably, no equivalent talent pool exists today for the study of Islamic extremism. In some cases, the security clearance process limits the Intelligence Community's ability to recruit analysts with contacts among relevant groups and with experience living overseas. Similarly, some security rules limit the ways in which analysts can develop substantive expertise. Finally, poor training or bad habits lead analysts to rely too much on secret information and to use nonclandestine and public information too little. Nonclandestine sources of information are critical to understanding societal, cultural, and political trends, but they are insufficiently utilized.

Lack of political context—and imagination. The October 2002 NIE contained an extensive technical analysis of Iraq's suspected weapons programs but little serious analysis of the socio-political situation in Iraq, or the motives and intentions of Iraqi leadership-

which, in a dictatorship like Iraq, really meant understanding Saddam. It seems unlikely to us that weapons experts used to combing reports for tidbits on technical programs would ever have asked: "Is Saddam bluffing?" or "Could he have decided to suspend his weapons programs until sanctions are lifted?" But an analyst steeped in Iraq's politics and culture at least *might* have asked those questions, and, of course, those turn out to be the questions that could have led the Intelligence Community closer to the truth. In that respect, the analysts displayed a lack of imagination. The Iraq example also reflects the Intelligence Community's increasing tendency to separate regional, technical, and (now) terrorism analysis—a trend that is being exacerbated by the gravitational pull toward centers like the National Counterterrorism Center (NCTC).

Overemphasis on and underperformance in daily intelligence products. As problematic as the October 2002 NIE was, it was not the Community's biggest analytic failure on Iraq. Even more misleading was the river of intelligence that flowed from the CIA to top policymakers over long periods of time—in the President's Daily Brief (PDB) and in its more widely distributed companion, the Senior Executive Intelligence Brief (SEIB). These daily reports were, if anything, more alarmist and less nuanced than the NIE. It was not that the intelligence was markedly different. Rather, it was that the PDBs and SEIBs, with their attention-grabbing headlines and drumbeat of repetition, left an impression of many corroborating reports where in fact there were very few sources. And in other instances, intelligence suggesting the existence of weapons programs was conveyed to senior policymakers, but later information casting doubt upon the validity of that intelligence was not. In ways both subtle and not so subtle, the daily reports seemed to be "selling" intelligence—in order to keep its customers, or at least the First Customer, interested.

Inadequate information sharing. There is little doubt that, at least in the context of counterterrorism, information sharing has improved substantially since September 11. This is in no small part due to the creation of the Terrorist Threat Integration Center (now NCTC) and the increased practice of housing collectors and analysts together, which provides a real-world solution to some of the bureaucratic and institutional barriers that exist between the big intelligence-collecting agencies. But in the three and a half years since September 11, this push to share information has not spread to other areas, including counterproliferation, where sharing is also badly needed. Furthermore, even in the counterterrorism context, information sharing still depends too much on physical co-location and personal relationships as opposed to integrated, Community-wide information networks. Equally problematic, individual departments and agencies continue to act as though they own the information they collect, forcing other agencies to pry information from them. Similarly, much information deemed "operational" by the CIA and FBI isn't routinely shared, even though analysts have repeatedly stressed its importance. All of this reveals that extensive work remains yet to be done.

Poor human intelligence. When the October 2002 NIE was written the United States had little human intelligence on Iraq's nuclear, biological, and chemical weapons programs and virtually no human intelligence on leadership intentions. While classification prevents us from getting into the details, the picture is much the same with respect to other dangerous threats. We recognize that espionage is always chancy at best; 50 years of pounding away at the Soviet Union resulted in only a handful of truly important human sources. Still, we have no choice but to do better. Old approaches to human intelligence alone are not the answer. Countries that threaten us are well aware of our human intelligence services' *modus operandi* and they know how to counter it. More of the same is unlikely to work. Innovation is

needed. The CIA deserves credit for its efforts to discover and penetrate the A.Q. Khan network, and it needs to put more emphasis on other innovative human intelligence methods.

Worse than having no human sources is being seduced by a human source who is telling lies. In fact, the Community's position on Iraq's biological weapons program was largely determined by sources who were telling lies—most notably a source provided by a foreign intelligence service through the Defense Intelligence Agency. Why DIA and the rest of the Community didn't find out that the source was lying is a story of poor asset validation practices and the problems inherent in relying on semi-cooperative liaison services. That the NIE (and other reporting) didn't make clear to policymakers how heavily it relied on a single source that no American intelligence officer had ever met, and about whose reliability several intelligence professionals had expressed serious concern, is a damning comment on the Intelligence Community's practices.

The challenge to traditional signals intelligence. Signals intelligence—the interception of radio, telephone, and computer communications—has historically been a primary source of good intelligence. But changes in telecommunications technology have brought new challenges. This was the case in Iraq, where the Intelligence Community lost access to important aspects of Iraqi communications, and it remains the case elsewhere. We offer a brief additional discussion of some of the modern challenges facing signals intelligence in our classified report, but we cannot discuss this information in an unclassified format.

Regaining signals intelligence access must be a top priority. The collection agencies are working hard to restore some of the access that they have lost; and they've had some successes. And again, many of these recent steps in the right direction are the result of innovative examples of cross-agency cooperation. In addition, successful signals intelligence will require a sustained research and development effort to bring cutting-edge technology to operators and analysts. Success on this front will require greater willingness to accept financial costs, political risks, and even human casualties.

Declining utility of traditional imagery intelligence against unconventional weapons programs. The imagery collection systems that were designed largely to work against the Soviet Union's military didn't work very well against Iraq's unconventional weapons program, and our review found that they aren't working very well against other priority targets, either. That's because our adversaries are getting better at denial and deception, and because the threat is changing. Again, we offer details about the challenges to imagery intelligence in our classified report that we cannot provide here.

Making the problem even more difficult, there is little that traditional imagery can tell us about chemical and biological facilities. Biological and chemical weapons programs for the most part can exist inside commercial buildings with no suspicious signatures. This means that we can get piles of incredibly sharp photos of an adversary's chemical factories, and we still will not know much about its chemical weapons programs. We can still see a lot and imagery intelligence remains valuable in many contexts, including support to military operations and when used in conjunction with other collection disciplines—but too often what we can see doesn't tell us what we need to know about nuclear, biological, and chemical weapons.

Measurement and signature intelligence (MASINT) is not sufficiently developed. The collection of technologies known as MASINT, which includes a virtual grab bag of advanced collection and analytic methods, is not yet making a significant contribution to

our intelligence efforts. In Iraq, MASINT played a negligible role. As in other contexts, we believe that the Intelligence Community should continue to pursue new technology aggressively—whether it is called MASINT, imagery, or signals intelligence. Innovation will be necessary to defeat our adversaries' denial and deception.

An absence of strong leadership. For over a year, despite unambiguous presidential direction, a turf battle raged between CIA's Counterterrorist Center (CTC) and the Terrorist Threat Integration Center (now NCTC). The two organizations fought over roles, responsibilities, and resources, and the Intelligence Community's leadership was unable to solve the problem. The intelligence reform act may put an end to this particular conflict, but we believe that the story reflects a larger, more pervasive problem within the Intelligence Community: the difficulty off making a decision and imposing the consequences on all agencies throughout the Community. Time and time again we have uncovered instances like this, where powerful agencies fight to a debilitating stalemate masked as consensus, because no one in the Community has been able to make a decision and then make it stick. The best hope for filling this gap is an empowered DNI.

LOOKING FORWARD: OUR RECOMMENDATIONS FOR CHANGE

Our case studies collectively paint a picture of an Intelligence Community with serious deficiencies that span the intelligence process. Stated succinctly, it has too little *integration* and too little *innovation* to succeed in the 21st century. It rarely adopts integrated strategies for penetrating high-priority targets; decisiomnakers lack authority to resolve agency disputes; and it develops too few innovative ways of gathering intelligence.

This section summarizes our major recommendations on how to change this state of affairs so that full value can be derived from the many bright, dedicated, and deeply committed professionals within the Intelligence Community. We begin at the top, and suggest how to use the opportunity presented by the new intelligence reform legislation to bring better integration and management to the Intelligence Community. Our management recommendations are developed in greater detail in Chapter Six of our report. We next offer recommendations that would improve intelligence collection (Chapter 7) and analysis (Chapter 8). Then we examine several specific and important intelligence challenges-improving information sharing (Chapter 9); integrating domestic and foreign intelligence in a way that both satisfies national security imperatives and safeguards civil liberties (Chapter 10); organizing the Community's counterintelligence mission (Chapter 11); and a largely classified chapter on managing covert action (Chapter 12). We then devote a stand-alone chapter to examining the most dangerous unconventional weapons challenges the Intelligence Community faces today and offer specific prescriptions for improving our intelligence capabilities against these threats (Chapter 13).

Leadership and Management: Forging an Integrated Intelligence Community

A former senior Defense Department official described today's Intelligence Community as "not so much poorly managed as unmanaged." We agree. Everywhere we looked, we found important (and obvious) issues of interagency coordination that went unattended, sensible Community-wide proposals blocked by pockets of resistance, and

critical disputes left to fester. Strong interagency cooperation was more likely to result from bilateral "treaties" between big agencies than from Community-level management. This ground was well-plowed by the 9/11 Commission and by several other important assessments of the Intelligence Community over the past decade.

In the chapter of our report devoted to management (Chapter 6), we offer detailed recommendations that we believe will equip the new Director of National Intelligence to forge today's loose confederation of 15 separate intelligence operations into a real, integrated Intelligence Community. A short summary of our more important management recommendations follows:

- ***Strong leadership and management of the Intelligence Community are indispensable.*** Virtually every senior intelligence official acknowledged the difficulty of leading and managing the Intelligence Community. Along with acting as the President's principal intelligence advisor, this will be the DNI's main job. His success in that job will determine the fate of many other necessary reforms. We thus recommend ways in which the DNI can use his limited, but not insignificant, authorities over money and people. No matter what, the DNI will not be able to run the Intelligence Community alone. He will need to create a management structure that allows him to see deep into the Intelligence Community's component agencies, and he will need to work closely with the other cabinet secretaries—especially the Secretary of Defense—for whom several Intelligence Community agencies also work. New procedures are particularly needed in the budget area, where today's Intelligence Community has a wholly inadequate Planning, Programming, and Budgeting System.
- ***Organize around missions.*** One of the most significant problems we identified in today's Intelligence Community is a lack of cross-Community focus on priority intelligence missions. By this, we mean that in most cases there is not one office, or one individual, who is responsible for making sure the Intelligence Community is doing all it can to collect and analyze intelligence on a subject like proliferation, or a country like Iran. Instead, intelligence agencies allocate their scarce resources among intelligence priorities in ways that seem sensible to them but are not optimal from a Community-wide perspective. The DNI needs management structures and processes that ensure a strategic, Community-level focus on priority intelligence missions. The specific device we propose is the creation of several "Mission Managers" on the DNI staff who are responsible for developing strategies for all aspects of intelligence relating to a priority intelligence target: the Mission Manager for China, for instance, would be responsible for driving collection on the China target, watching over China analysis, and serving as a clearinghouse for senior policymakers seeking China expertise.
- ***Establish a National Counter Proliferation Center.*** The new intelligence legislation creates one "national center"—the National Counterterrorism Center (NCTC)—and suggests the creation of a second, similar center devoted to counterproliferation issues. We agree that a National Counter Proliferation Center (NCPC) should be established but believe that it should be fundamentally different in character from the NCTC. The NCTC is practically a separate agency; its large staff is responsible not only for conducting counterterrorism analysis and intelligence gathering but also for "strategic operational planning" in support of counterterrorism policy. In contrast, we

believe that the NCPC should be a relatively small center (i.e., fewer than 100 people); it should primarily play a *management and coordination* function by overseeing analysis and collection on nuclear, biological, and chemical weapons across the Intelligence Community. In addition, although we agree that government-wide strategic planning is required to confront proliferation threats, we believe that entities other than the NCPC—such as a Joint Interagency Task Force we propose to coordinate interdiction efforts—should perform this function.

- ***Build a modern workforce.*** The intelligence reform legislation grants the DNI substantial personnel authorities. In our view, these authorities come none too soon. The Intelligence Community has difficulty recruiting and retaining individuals with critically important skill sets—such as technical and scientific expertise, and facility with foreign languages—and has not adapted well to the diverse cultures and settings in which today's intelligence experts must operate. We propose the creation of a new human resources authority in the Office of the DNI to develop Community-wide personnel policies and overcome these systemic shortcomings. We also offer specific proposals aimed at encouraging "joint" assignments between intelligence agencies, improving job training at all stages of an intelligence professional's career, and building a better personnel incentive structure.
- ***Create mechanisms for sustained oversight from outside the Intelligence Community—and for self-examination from the inside.*** Many sound past proposals for intelligence reform have withered on the vine. Either the Intelligence Community is inherently resistant to outside recommendations, or it lacks the institutional capacity to implement them. In either case, sustained external oversight is necessary. We recommend using the new Joint Intelligence Community Council—which comprises the DNI and the cabinet secretaries with intelligence responsibilities—as a high-level "consumer council." We also recommend the President's Foreign Intelligence Advisory Board play a more substantial advisory role. Like others before us, we suggest that the President urge Congress to reform its own procedures to provide better oversight. In particular, we recommend that the House and Senate intelligence committees create focused oversight subcommittees, that the Congress create an intelligence appropriations subcommittee and reduce the Intelligence Community's reliance on supplemental funding, and that the Senate intelligence committee be given the same authority over joint military intelligence programs and tactical intelligence programs that the House intelligence committee now exercises. Finally—and perhaps most importantly—we recommend that the DNI create mechanisms to ensure that the Intelligence Community conducts "lessons learned" and after-action studies so that it will be better equipped to identify its *own* strengths and weaknesses.

Additional Leadership and Management Recommendations

In addition to those described above, Chapter Six of our report offers recommendations concerning:

- How to build a coordinated process for "target development"—that is, the directing of collection resources toward priority intelligence subjects;

- How to spur innovation outside individual collection agencies;
- How the DNI might handle the difficult challenges of integrating intelligence from at home and abroad, and of coordinating activities and procedures with the Department of Defense; and
- How the DNI might organize the office of the DNI to fit needed leadership and management functions into the framework created by the intelligence reform legislation.

Integrated and Innovative Collection

The intelligence failure in Iraq did not begin with faulty analysis. It began with a sweeping collection failure. The Intelligence Community simply couldn't collect good information about Iraq's nuclear, biological, or chemical programs. Regrettably, the same can be said today about other important targets, none of which will ever be easy targets—but we can and should do better.

Urging each individual collection agency to do a better job is not the answer. Where progress has been made against such targets, the key has usually been more integration and more innovation in collecting intelligence. As a result, we recommend the following:

- ***Create a new Intelligence Community process for managing collection as an "integrated enterprise."*** In order to gather intelligence effectively, the Intelligence Community must develop and buy sophisticated technical collection systems, create strategies for focusing those systems on priority targets, process and exploit the data that these systems collect, and plan for the acquisition of future systems. Today, each of these functions is performed primarily within individual collection agencies, often with little or no Community-level direction or interagency coordination. We propose that the DNI create what we call an "integrated collection enterprise" for the Intelligence Community—that is, a management structure in which the Community's decentralized collection capabilities are harmonized with intelligence priorities and deployed in a coordinated way.
- ***Create a new Human Intelligence Directorate.*** Both the Defense Department and the FBI are substantially increasing their human intelligence activities abroad, which heightens the risk that intelligence operations will not be properly coordinated with the CIA's human espionage operations, run by its Directorate of Operations (DO). The human intelligence activities of the Defense Department and the FBI should continue, but in the world of foreign espionage, a lack of coordination can have dangerous, even fatal, consequences. To address this pressing problem, we suggest the creation of a new Human Intelligence Directorate within the CIA, to which the present DO would be subordinate, to ensure the coordination of all U.S. agencies conducting human intelligence operations overseas. In addition to this coordination role, the Human Intelligence Directorate would serve as the focal point for Community-wide human intelligence issues, including helping to develop a national human intelligence strategy, broadening the scope of human intelligence activities, integrating (where appropriate) collection and reporting systems, and establishing Community-wide standards for training and tradecraft.

- ***Develop innovative human intelligence techniques.*** The CIA's Directorate of Operations is one of the Intelligence Community's elite and storied organizations. However, the DO has remained largely wedded to the traditional model—a model that does not meet the challenges posed by terrorist organizations and nations that are "denied areas" for U.S. personnel. Accordingly, we recommend the establishment of an "Innovation Center" within the CIA's new Human Intelligence Directorate—but *not* within the DO. This center would spur the use of new and nontraditional methods of collecting human intelligence. In the collection chapter of our report, we also detail several new methods for collecting human intelligence that in our judgment should either be explored or used more extensively.
- ***Create an Open Source Directorate within the CIA.*** We are convinced that analysts who use open source information can be more effective than those who don't. Regrettably, however, the Intelligence Community does not have an entity that collects, processes, and makes available to analysts the mass of open source information that is available in the world today. We therefore recommend the creation of an Open Source Directorate at the CIA. The directorate's mission would be to deploy sophisticated information technology to make open source information available across the Community. This would, at a minimum, mean gathering and storing digital newspapers and periodicals that are available only temporarily on the Internet and giving Intelligence Community staff easy (and secure) access to Internet materials. In addition, because we believe that part of the problem is analyst resistance, not lack of collection, we recommend that some of the new analysts allocated to CIA be specially trained to use open sources and then to act as open source "evange-analysts" who can jumpstart the open source initiative by showing its value in addressing particular analytic problems. All of this, we believe, will help improve the Intelligence Community's surprisingly poor "feel" for cultural and political issues in the countries that concern policymakers most. The Open Source Directorate should also be the primary test bed for new information technology because the security constraints—while substantial—are lower for open source than for classified material.
- ***Reconsider MASINT.*** Measurements and signatures can offer important intelligence about nuclear, biological, and chemical weapons. But the tools we use to collect these measurements and signatures—tools collectively referred to within the intelligence community as "MASINT"—do not obviously constitute a single discipline. In a world of specialized collection agencies, there is reason to suspect that these orphaned technologies may have been under-funded and under-utilized. We recommend that the DNI take responsibility for developing and coordinating new intelligence technologies, including those that now go under the title MASINT. This could be done by a special coordinator, or as part of the DNI's Office of Science and Technology. The DNI's office does not need to directly control MASINT collection. Rather, we recommend that individual collection agencies assume responsibility for aspects of MASINT that fall naturally into their bailiwicks. At the same time, the DNI's designated representative would promote and monitor the status of new technical intelligence programs throughout the Intelligence Community to ensure that they are fully implemented and given the necessary attention.

Additional Collection Recommendations

In addition to those described above, Chapter Seven of our report offers recommendations concerning:

- Developing new human and technical collection methods;
- Professionalizing human intelligence across the Intelligence Community;
- Creating a larger and better-trained human intelligence office cadre;
- Amending the Foreign Intelligence Surveillance Act to extend the duration of certain forms of electronic surveillance against non-U.S. persons, to ease administrative burdens on NSA and the Department of Justice; and
- Improving the protection of sources and methods by reducing authorized and unauthorized disclosures.

Transforming Analysis

Integrated, innovative collection is just the beginning of what the Intelligence Community needs. Some of the reforms already discussed, particularly the DNI-level "Mission Managers," will improve analysis. But much more is needed. In particular, analytic expertise must be deepened, intelligence gaps reduced, and existing information made more usable—all of which would improve the quality of intelligence.

As an overarching point, however, the Intelligence Community must recognize the central role of analysts in the intelligence process. Needless to say, analysts are the people who analyze intelligence, put it in context, and communicate the intelligence to the people who need it. But in addition, analysts are the repositories for what the Intelligence Community *doesn't* know, and they must clearly convey these gaps to decisionmakers—as well as to collectors so that the Intelligence Community does everything it can to fill the holes. (Analysts will also play an increasingly prominent role in information security, as they "translate" intelligence from the most sensitive of sources to a variety of consumers, ranging from state and local first responders to senior policymakers.) To enable analysts to fulfill these roles, we recommend the following:

- ***Empower Mission Managers to coordinate analytic efforts on a given topic.*** The Mission Managers we propose would serve as the focal point for all aspects of the intelligence effort on a particular issue. They would be aware of the analytic expertise in various intelligence agencies, assess the quality of analytic products, identify strategic questions receiving inadequate attention, encourage alternative analysis, and ensure that dissenting views are expressed to intelligence users. When necessary, they would recommend that the DNI use his personnel authorities to move analysts to priority intelligence topics. At the same time, Mission Managers should *not* be responsible for providing a single, homogenized analytic product to decisionmakers; rather, Mission Managers should be responsible for encouraging alternative analysis and for ensuring that dissenting views are expressed to intelligence customers. In sum, Mission Managers should be able to find the right people and expertise and make sure that the right analysis, including alternative analysis, is getting done.

- ***Strengthen long-term and strategic analysis.*** The most common complaint we heard from analysts in the Intelligence Community was that the pressing demand for current intelligence "eats up everything else." Analysts cannot maintain their expertise if they cannot conduct long-term and strategic analysis. Because this malady is so pervasive and has proven so resistant to conventional solutions, we recommend establishing an organization to perform only long-term and strategic analysis under the National Intelligence Council, the Community's existing focal point for interagency long-term analytic efforts. The new unit could serve as a focal point for Community-wide alternative analysis, thereby complementing agency-specific efforts at independent analysis. And although some analysts in this organization would be permanently assigned, at least half would serve only temporarily and would come from all intelligence agencies, including NGA and NSA, as well as from outside the government. Such rotations would reinforce good tradecraft habits, as well as foster a greater sense of Community among analysts and spur collaboration on other projects.
- ***Encourage diverse and independent analysis.*** We believe that diverse and independent analysis—often referred to as "competitive analysis"—should come from many sources. As we have just noted, we recommend that our proposed long-term research and analysis unit, as well as the National Intelligence Council, conduct extensive independent analysis. In some circumstances there is also a place for a "devil's advocate"—someone appointed to challenge the consensus view. We also think it important that a not-for-profit "sponsored research institute" be created *outside* the Intelligence Community; such an institute would serve as a critical window into outside expertise, conduct its own research, and reach out to specialists, including academics and technical experts, business and industry leaders, and representatives from the nonprofit sector. Finally, the Intelligence Community should encourage independent analysis throughout its analytic ranks. In our view, this can best be accomplished through the preservation of dispersed analytic resources (as opposed to consolidation in large "centers"), active efforts by Mission Managers to promote independent analysis, and Community-wide training that instills the importance of such analysis.
- ***Improve the rigor and "tradecraft" of analysis.*** Our studies, and many observers, point to a decline in analytic rigor within the Intelligence Community. Analysts have suffered from weak leadership, insufficient training, and budget cutbacks that led to the loss of our best, most senior analysts. There is no quick fix for tradecraft problems. However, we recommend several steps: increasing analyst training; ensuring that managers and budget-writers allot time and resources for analysts to actually *get* trained; standardizing good tradecraft practices through the use of a National Intelligence University; creating structures and practices that increase competitive analysis; increasing managerial training for Intelligence Community supervisors; enabling joint and rotational assignment opportunities; ensuring that finished intelligence products are sufficiently transparent so that an analyst's reasoning is visible to intelligence customers; and implementing other changes in human resource policies—such as merit-based-pay—so that the best analysts are encouraged to stay in government service.
- ***Communicating intelligence to policymakers.*** The best intelligence in the world is worthless unless it is effectively and accurately communicated to those who need it.

The Iraq weapons of mass destruction case is a stark example. The daily reports sent to the President and senior policymakers discussing Iraq over many months proved to be disastrously one-sided. We thus offer recommendations on ways in which intelligence products can be enhanced, including how the President's Daily Brief (PDB) might be improved. In this regard, we suggest the elimination of the inherently misleading "headline" summaries in PDBs and other senior policymaker briefs, and that the DNI oversee production of the PDB. To accomplish this, we recommend the DNI create an analytic staff too small to routinely undertake drafting itself, but large enough to have background on many of the issues that are covered by the PDB. The goal would be to enable the DNI to coordinate and oversee the process, without requiring him to take on the heavy—and almost overwhelming—mantle of daily intelligence support to the President. Critically, the DNI's staff would also ensure that the PDB reflects alternative views from the Community to the greatest extent feasible.

We also recommend that the DNI take responsibility, with the President's concurrence, for the three primary sources of intelligence that now reach the President: the PDB, the President's Terrorism Threat Report—a companion publication produced by the NCTC and focused solely on terrorism-related issues—and the briefing by the Director of the FBI. We suggest that the DNI coordinate this intelligence in a manner that eliminates redundancies and ensures that only material that is necessary for the President be included. We think this last point is especially important because we have observed a disturbing trend whereby intelligence is passed to the President (as well as other senior policymakers) not because it requires high-level attention, but because passing the information "up the chain" provides individuals and organizations with bureaucratic cover.

- ***Demand more from analysts.*** We urge that policymakers actively probe and question analysts. In our view, such interaction is not "politicization." Analysts should expect such demanding and aggressive testing without—as a matter of principle and professionalism—allowing it to subvert their judgment.

Additional Analysis Recommendations

In addition to those described above, Chapter Eight of our report offers recommendations concerning:

- Developing technologies capable of exploiting large volumes of foreign language data without the need for human translations;
- Improving career-long analytical and managerial training;
- Creating a database for all finished intelligence, as well as adopting technology to update analysts and decisionmakers when intelligence judgments change;
- Improving the Intelligence Community's science, technology, and weapons expertise;
- Changing the way analysts are hired, promoted, and rewarded; and
- Institutionalizing "lessons learned" procedures to learn from past analytical successes and failures.

Information Sharing

While the new intelligence reform legislation correctly identifies information sharing as an area where major reforms are necessary, the steps it takes to address the problem raise as many questions as they answer. The legislation creates a new position—a "Program Manager" who sits outside of the Intelligence Community and reports directly to the President—responsible for creating an integrated, government-wide Information Sharing Environment for all "terrorism information." At the same time, the Director of National Intelligence is given responsibility for facilitating information sharing for *all* intelligence information *within* the Intelligence Community.

We believe that these two separate statutory information sharing efforts should be harmonized. We are less confident that any particular mechanism is optimal. Perhaps the least bad solution to this tricky problem—short of new legislation—is to require that the Program Manager report to the President *through* the DNI, and that the Information Sharing Environment be expanded to include all intelligence information, not just intelligence related to terrorism. In recommending this solution, however, we emphasize that information sharing cannot be understood merely as an Intelligence Community endeavor; whoever leads the effort to build the Information Sharing Environment must be sensitive to the importance of distributing necessary information to those who need it both in the non-intelligence components of the federal government, and to relevant state, local, and tribal authorities.

We also make specific recommendations concerning how best to implement the information sharing effort. Among these recommendations are: designating a single official under the DNI who will be responsible for both information sharing *and* information security, in order to break down cultural and policy barriers that have impeded the development of a shared information space; applying advanced technologies to the Information Sharing Environment to permit more expansive sharing with far greater security protections than currently exist in the Intelligence Community; and establishing clear and consistent Community-wide information sharing and security policies. Last but not least, we recommend that the DNI jettison the phrase "information sharing" itself, which merely reinforces the (incorrect) notion that information is the property of individual intelligence agencies, rather than of the government as a whole.

Finally, we believe it is essential to note the importance of protecting civil liberties in the context of information sharing. We believe that the intelligence reform act provides the framework for appropriate protection of civil liberties in this area, and that all information sharing must be done in accordance with Attorney General guidelines relating to "U.S. persons" information. At the same time, in our view the pursuit of privacy and national security is *not* a zero-sum game. In fact, as we describe in our report, many of the very same tools that provide counterintelligence protection can be equally valuable in protecting privacy.

Intelligence at Home: the FBI, Justice, and Homeland Security

Although the FBI has made strides in turning itself into a true collector and analyst of intelligence, it still has a long way to go. The Bureau, among other things, has set up Field Intelligence Groups in each of its 56 field offices and created an Executive Assistant Director for Intelligence with broad responsibility for the FBI's intelligence mission. Yet

even FBI officials acknowledge that its collection and analysis capabilities will be a work in progress until at least 2010.

In our view, the biggest challenge is to make the FBI a full participant in the Intelligence Community. This is not just a matter of giving the Bureau new resources and new authority. It must also mean integrating the FBI into a Community that is subject to the DNI's coordination and leadership. Unfortunately, the intelligence reform legislation leaves the FBI's relationship to the DNI especially murky. We recommend that the President make clear that the FBI's intelligence activities are to be fully coordinated with the DNI and the rest of the Community.

- ***Create a separate National Security Service within the FBI that includes the Bureau's Counterintelligence and Counterterrorismi Divisions, as well as the Directorate of Intelligence.*** The intelligence reform act empowers the DNI to lead the Intelligence Community, which includes the FBI's "intelligence elements." Although the statute leaves the term ambiguous, we believe that "elements" must include *all* of the Bureau's national security-related components—the Intelligence Directorate *and* the Counterterrorism and Counterintelligence Divisions. Anything less and the DNI's ability to coordinate intelligence across our nation's borders will be dangerously inadequate.

  Simply granting the DNI authority over the Bureau's current Directorate of Intelligence is, we believe, insufficient. We say this because the Directorate of Intelligence has surprisingly little operational, personnel, and budgetary authority. Currently the directorate has no authority to initiate, terminate, or re-direct any collection or investigative operation in any of the FBI's 56 regional field offices that are scattered throughout the nation or within any of the four operational divisions (Counterintelligence, Counterterrorism, Cyber, and Criminal) at FBI Headquarters. Although the Directorate of Intelligence may "task" the field offices to collect against certain requirements, it has no direct authority to ensure that FBI resources actually carry out these requirements. Its "taskings" are really "askings." Nor does the directorate contain the great bulk of the FBI's intelligence analysts. And the directorate has no clear control over the Bureau's portion of the National Intelligence Program budget, which is largely spent by the Counterterrorism and Counterintelligence Divisions. In short, the intelligence directorate has few, if any, mechanisms for exercising direct authorities over FBI's intelligence collectors or analytic products. With a direct line of authority only to the Bureau's Directorate of Intelligence, the DNI cannot be ensured influence over the Bureau's national security functions, and the FBI will not be fully integrated into the Intelligence Community.

  We therefore recommend the creation of a separate National Security Service *within the FBI* that has full authority to manage, direct, and control all Headquarters and Field Office resources engaged in counterintelligence, counterterrorism, and foreign intelligence collection, investigations, operations, and analysis. Critically, this division would then be subject to the same DNI authorities as apply to such Defense agencies as NSA and NGA. Of equal importance, this structure would maintain the Attorney General's oversight of the FBI's activities to ensure the Bureau's compliance with U.S. law. In this sense, the Attorney General's role would be similar to that of the Secretary of Defense, who—even with the appointment of

the DNI—continues to oversee Defense Department agencies within the Intelligence Community, like NSA and NGA.

- ***Ensure better mechanisms for coordination and cooperation on foreign intelligence collection in the United States.*** The expansion of the FBI's intelligence collection and reporting activities over the past few years has engendered turf battles between the CIA and the FBI that have already caused counterproductive conflicts both within and outside of the United States. In particular, the two agencies have clashed over the domestic collection of foreign intelligence—an area in which they have long shared responsibilities. We see no reason to change the status quo dramatically or to expand the FBI's authority over foreign intelligence gathering inside the United States. If unanticipated conflicts emerge, both agencies should be instructed to take their differences to the DNI for resolution. The two agencies' capabilities should complement, rather than compete with, one another. We also expect that such an integrated approach would continue to rely on the existing Attorney General guidelines, which carefully limit the way both agencies operate within the United States, and with regard to U.S. persons overseas. We believe that strong CIA/FBI cooperation and clear guidelines are essential for protection of civil liberties as well as for effective intelligence gathering.
- ***Reorient the Department of Justice.*** Every agency that has major responsibility for terrorism and intelligence has been overhauled in the past four years. With one exception: at the Department of Justice, the famous "wall" between intelligence and criminal law still lingers, at least on the organization charts. On one side is the Office of Intelligence Policy and Review, which handles Foreign Intelligence Surveillance Court orders—those court orders that permit wiretaps and physical searches for national security reasons. On the other side are two separate sections of the Criminal Division (Counterterrorism and Counterespionage), reporting to two separate Deputy Assistant Attorneys General. This organizational throwback to the 1990s scatters intelligence expertise throughout the Department and in some cases has contributed to errors that hampered intelligence gathering. A single office with responsibility for counterterrorism, counterintelligence, and intelligence investigations would ensure better communication and reduce the tendency to rebuild the wall along bureaucratic lines.

  We recommend that these three components (perhaps joined by a fourth Justice Department component that coordinates issues related to transnational crimes) be placed together under the authority of an Assistant Attorney General for National Security who would, like the Assistant Attorney General for the Criminal Division, report either directly to the Deputy Attorney General, or to a newly created Associate Attorney General responsible for both the National Security and Criminal Divisions.
- ***Strengthen the Department of Homeland Security's relationship with the Intelligence Community.*** The Department of Homeland Security is the primary repository of information about what passes in and out of the country—a critical participant in safeguarding the United States from nuclear, biological, or chemical attack. Yet, since its inception, Homeland Security has faced immense challenges in collecting information effectively, making it available to analysts and users both inside and outside the Department, and bringing intelligence support to law enforcement and first responders who seek to act on such information. We did not

conduct a detailed study of Homeland Security's capabilities, but it is clear to us that the department faces challenges in all four roles it plays in the intelligence community—as collector, analyst, disseminator, and customer.

Among the obstacles confronting Homeland Security, we found during the course of our study that the Department's Immigration and Customs Enforcement still operates under an order inherited from the Treasury Department in the 1980s. The order requires high-level approval for virtually all information sharing and assistance to the Intelligence Community. We think this order should be rescinded, and we believe the DNI should carefully examine how Homeland Security works with the rest of the Intelligence Community.

COUNTERINTELLIGENCE

Every intelligence service on the planet wants to steal secrets from the last remaining superpower. But as other nations increase their intelligence operations against the United States, U.S. counterintelligence has been in a defensive crouch—fractured, narrowly focused, and lacking national direction. This may change as a result of the President's newly announced counterintelligence strategy. The good ideas in the strategy must, however, still be put into practice.

CIA does counterintelligence abroad, but its capabilities are limited. The FBI's counterintelligence efforts within the United States are well-staffed, but hardly strategic in their nature. Finally, the Defense Department's counterintelligence capabilities lack effective cross-department integration and direction. To address these concerns, we recommend four steps to strengthen counterintelligence: the empowerment of the nation's chief counterintelligence officer, the National Counterintelligence Executive (NCIX); the development of a new CIA capability for enhancing counterintelligence abroad; the centralization of the Defense Department's counterintelligence functions; and, as suggested earlier, bringing the FBI into the Intelligence Community to ensure that its robust counterintelligence capabilities are employed in line with the DNI's priorities. Moreover, all of these efforts must focus greater attention on the technical aspects of counterintelligence, as our adversaries shift from human spying to attempting to penetrate our information infrastructure.

COVERT ACTION

If used in a careful and limited way, covert action can serve as a more subtle and surgical tool than forms of acknowledged employment of U.S. power and influence. As part of our overall review of the Intelligence Community, we conducted a careful study of U.S. covert action capabilities. Our findings were included in a short, separate chapter of our classified report. Regrettably, this area is so heavily classified that we could not include a chapter on the subject in our unclassified report.

We will, however, state here—at a necessarily high level of generality—some of our overall conclusions on covert action. At the outset, we note that we found current covert action programs in the counterproliferation and counterterrorism areas to be energetic, innovative, and well-executed within the limits of their authority and funding. Yet some critically important programs are hobbled by lack of sustained strategic planning, in-

sufficient commitment of resources on a long-term basis, and a disjointed management structure. In our classified report we suggest organizational changes that we believe would consolidate support functions for covert action and improve the management of covert action programs within the Intelligence Community; we are unable to provide further details on these recommendations, however, in this unclassified format.

Addressing Proliferation

So far, we have focused on improving the Intelligence Community writ large—on the theory that only a redesigned Community can substantially improve its performance in assessing the threat posed by weapons of mass destruction. But quite apart from the structural changes we have already recommended, the Intelligence Community also needs to change the way it approaches two of the greatest threats—biological weapons and new forms of nuclear proliferation.

BIOLOGICAL WEAPONS

The 2001 anthrax attacks on the United States killed five people, crippled mail delivery in several cities for a year, and imposed more than a billion dollars in decontamination costs. For all that, we were lucky. Biological weapons are cheaper and easier to acquire than nuclear weapons—and they could be more deadly. The threat is deeply troubling today; it will be more so tomorrow, when genetic modification techniques will allow the creation of even worse biological weapons. Most of the traditional Intelligence Community collection tools are of little or no use in tackling biological weapons. In our classified report, we discuss some of the specific challenges that confront our intelligence effort against the biological threat—but regrettably we cannot discuss them here.

Faced with a high-priority problem that does not yield to traditional methods, large parts of the Intelligence Community seem to have lowered their expectations and focused on other priorities. This is unacceptable. The Intelligence Community, and the government as a whole, needs to approach the problem with a new urgency and new strategies:

- ***Work with the biological sciences community.*** The Intelligence Community simply does not have the in-depth technical knowledge about biological weapons that it has about nuclear weapons. To close the expertise gap, the Community cannot rely on hiring biologists, whose knowledge and skills are extremely important, but whose depth and timeliness of expertise begins eroding as soon as they move from the laboratory to the intelligence profession. Instead, the DNI should create a Community Biodefense Initiative to institutionalize outreach to technical experts inside and outside of government. We describe specific components of this initiative in the body of our report.
- ***Make targeted collection of biological weapons intelligence a priority within the Intelligence Community.*** The Intelligence Community's collection woes starkly illustrate the need for more aggressive, targeted approaches to collection on biological threats. We recommend that the DNI create a deputy within the National Counter Proliferation Center who is specifically responsible for biological weapons; this deputy would ensure the implementation of a comprehensive biological weapons targeting strategy, which would entail gaining real-time access to non-

traditional sources of information, filtering open source data, and devising specific collection initiatives directed at the resulting targets.

- ***Leverage regulation for biological weapons intelligence.*** The United States should look outside of intelligence channels for enforcement mechanisms that can provide new avenues of international cooperation and resulting opportunities for intelligence collection on biological threats. In the corresponding chapter of our report, we recommend encouraging foreign criminalization of biological weapons development and establishing biosafety and biosecurity regulations under United Nations Security Council Resolution 1540. We also propose extending biosecurity and biosafety regulations to foreign institutions with commercial ties to the United States.

NUCLEAR WEAPONS

The intelligence challenge posed by nuclear weapons continues to evolve. The Intelligence Community must continue to monitor established nuclear states such as Russia and China, and at the same time face newer and potentially more daunting challenges like terrorist use of a nuclear weapon. But the focus of the U.S. Intelligence Community has historically been on the capabilities of large nation states. When applied to the problem of terrorist organizations and smaller states, many of our intelligence capabilities are inadequate.

The challenges posed by the new environment are well-illustrated by two aspects of nuclear proliferation. The first is the continuing challenge of monitoring insecure nuclear weapons and materials, or "loose nukes"—mainly in the former Soviet Union but also potentially in other nations. The second aspect is the appearance of non-state nuclear "brokers," such as the private proliferation network run by the Pakistani scientist A.Q. Khan. In Khan's case, innovative human intelligence efforts gave the United States access to this proliferation web. However, not only does the full scope of Khan's work remain unknown, but senior officials readily acknowledge that the Intelligence Community must know more about the private networks that support proliferation. The Intelligence Community must adapt to the changing threat.

INTELLIGENCE SUPPORT TO INTERDICTION

So far, the Intelligence Community has enjoyed a number of successes intercepting materials related to nuclear, biological, and chemical weapons (and their related delivery systems)—the process commonly referred to as "interdiction." But success has come at a cost. The Intelligence Community has focused so much energy on its own efforts that the Community shows less ambition and imagination in supporting other agencies that should play a large role in interdiction. Many other federal agencies could do more to interdict precursors, weapons components, and dangerous agents if they had effective intelligence support. We recommend several mechanisms to improve intelligence support to these agencies, most particularly the creation of a counterproliferation Joint Interagency Task Force modeled on similar entities that have proved successful in the counternarcotics context.

Moreover, since it may not be possible in all cases to identify proliferation shipments before they reach the United States, our last line of defense is detecting and stopping these

shipments before they reach our border. Yet new sensor technologies have faced challenges. In the corresponding chapter of this report, we suggest how the Intelligence Community and Department of Homeland Security can work together on this issue.

LEVERAGING LEGAL AND REGULATORY MECHANISMS

Intelligence alone cannot solve the proliferation threat. But it may not have to. Information that spies and eavesdroppers would spend millions for and risk their lives to steal can sometimes be easily obtained by the right Customs, Treasury, or export control officials. The industries that support proliferation are subject to a host of regulatory regimes. But the agencies that regulate industry in these areas—Treasury, State, Homeland Security, and Commerce—do not think of themselves as engaged in the collection of intelligence, and the Intelligence Community only rarely appreciates the authorities and opportunities presented by regulatory regimes.

Given the challenges presented by quasi-governmental proliferation, the United States must leverage all of its capabilities to flag potential proliferators, gain insight into their activities, and interdict them, where appropriate. We therefore recommend a series of possible changes to existing regulatory regimes, all designed to improve insight into nuclear, biological, or chemical proliferation and enhance our ability to take action. These changes include negotiating ship boarding agreements that include tagging and tracking provisions to facilitate the surveillance of suspect vessels, taking steps to facilitate greater coordination between the Commerce Department (and Immigrations and Customs Enforcement) and the Intelligence Community, using Commerce Department and Customs and Border Protection regulations to facilitate information sharing about suspect cargo and persons and to justify related interdictions, and expanding the Treasury Department's authority to block assets of proliferators.

CONCLUSION

The harm done to American credibility by our all too public intelligence failings in Iraq will take years to undo. If there is good news it is this: without actually suffering a massive nuclear or biological attack, we have learned how badly the Intelligence Community can fail in struggling to understand the most important threats we face. We must use the lessons from those failings, and from our successes as well, to improve our intelligence for the future, and do so with a sense of urgency. We already have thousands of dedicated officers and many of the tools needed to do the job. With that in mind, we now turn first to what went wrong in Iraq, then to other intelligence cases, and finally to our detailed recommendations for action.

APPENDIX G

THE BUTLER REPORT ON WEAPONS OF MASS DESTRUCTION IN IRAQ, 2004

Editor's note: The British conducted their own inquiry into why its secret services—like the U.S. intelligence agencies—failed to estimate accurately that Saddam Hussein had abandoned his WMD program. Led by The Rt Hon Lord Butler of Brockwell KG GCB CVO, the British panel reported on July 14, 2004. It key findings related to intelligence and counterterrorism are presented below.

CHAPTER 1
THE NATURE AND USE OF INTELLIGENCE

> "Much of the intelligence that we receive in war is contradictory, even more of it is plain wrong, and most of it is fairly dubious. What one can require of an officer, under these circumstances, is a certain degree of discrimination, which can only be gained from knowledge of men and affairs and from good judgement. The law of probability must be his guide."
>
> [Clausewitz, On War, Vol 1, Bk 1, Ch VI]

1.1 INTRODUCTION

20. In view of the subject matter of our Review, and of what we have found in the course of it, we think that it may be helpful to the general reader to describe the nature of intelligence; the successive processes of validation, analysis and assessment which are necessary for using it properly; its limitations; and the risks which nevertheless remain.

Source: "Review of Intelligence on Weapons of Mass Destruction," *Report of a Committee of Privy Counsellors*, Chairman: Lord Butler, HC 898 (July 14, 2004), pp. 7–16, 29–36.

21. Governmental decisions and actions, at home and abroad, are based on many types of information. Most is openly available or compiled, much is published, and some is consciously provided by individuals, organisations or other governments in confidence. A great deal of such information may be accurate, or accurate enough in its own terms. But equally much is at best uninformed, while some is positively intended to mislead. To supplement their knowledge in areas of concern where information is for one reason or another inadequate, governments turn to secret sources. Information acquired against the wishes and (generally) without the knowledge of its originators or possessors is processed by collation with other material, validation, analysis and assessment and finally disseminated as 'intelligence.' To emphasise the point, the term 'secret intelligence' is often used (as, for instance, enshrined in the title of the Secret Intelligence Service), but in this Review we shall use the simple word 'intelligence.'
22. The protective security barriers which intelligence collectors have to penetrate are usually formidable, and particularly so in the case of programmes which are the subject of this Review. Nuclear, biological and chemical programmes are amongst the ultimate state secrets, controlled by layers of security protection going beyond those applied to conventional weapons. Those of the greatest concern to governments are usually embedded within a strong apparatus of state control. Few of the many people who are necessarily involved in such programmes have a view of more than their own immediate working environment, and very few have comprehensive knowledge of the arrangements for the control, storage, release and use of the resulting weapons. At every stage from initial research and development to deployed forces, nuclear, biological and chemical weapons and their delivery systems are treated as being of particular sensitivity, often to the extent of the establishment of special command and control arrangements in parallel with, but separate from, normal state or military channels.

1.2 COLLECTION

23. The UK has three intelligence and security agencies ('the agencies') responsible for the collection of intelligence[1]: the Secret Intelligence Service (SIS), the Security Service and Government Communications Headquarters (GCHQ). The Defence Intelligence Staff (DIS), part of the Ministry of Defence (MOD), also manages some intelligence collection, notably that of imagery, but its main function is all-source analysis and assessment and the production of collated results, primarily to serve MOD requirements.
24. There is a panoply of collection techniques to acquire intelligence which do not exactly correspond to inter-departmental organisational boundaries. The three main ones are signals intelligence (the product of interception, generally abbreviated to 'Sigint'); information from human sources such as classical espionage agents (which is conveniently described, by extension from the previous category, as 'Humint'): and photography, or more generally imagery ('Imint'). Signals intelligence and human intelligence are of widespread and general applicability. They can produce intelligence on any topic (for example, the intentions, plans, negotiations, activities and achievements of people involved in the development, acquisition, deployment and use of unconventional weapons), since ultimately the data they acquire stem from the

[1] They also have other functions not relevant here.

human beings involved. Imagery is more confined to the study of objects (buildings, aircraft, roads, topography), though modern techniques have extended its abilities (for example, infra-red photography can in some circumstances show where an object was, even though it may have gone by the time the photograph is taken).

25. There are also other, more specialised intelligence techniques, some of particular relevance to this Review[2]. For example, the development of nuclear explosives inevitably involves highly-radioactive materials, radiation from which may be detected. Leakage from facilities concerned with the development of chemical and biological agents, and deposits in testing areas, can provide characteristic indicators. Missile testing may involve the generation of considerable heat, which can be detected, and missiles may be tracked by radar.

26. In the case of the weapons covered by this Review, there is additionally another category of information which is frequently mentioned by the Joint Intelligence Committee (JIC) in its assessments. International inspection and enforcement bodies have been established, on a permanent basis (e.g. the International Atomic Energy Agency), or temporary basis (e.g. the United Nations Special Commission), to ensure compliance with international treaties or United Nations resolutions[3]. Some of the findings and reports of these bodies are published on an official basis to United Nations members and are of considerable importance. In Iraq between 1991 and 1998, in many ways they surpassed anything that national intelligence agencies could do, but since their work is carried out on behalf of the United Nations it can hardly be considered 'intelligence' by the definitions to which we are working. Data obtained in the course of work on export licensing can also be important.

1.3 VALIDATION

27. Intelligence, though it may not differ in type or, often, reliability from other forms of information used by governments, operates in a field of particular difficulty. By definition the data it is trying to provide have been deliberately concealed. Before the actual content of an intelligence report can be considered, the validity of the process which has led to its production must be confirmed. For imagery and signals intelligence this is not usually an issue, although even here the danger of deception must be considered. But for human intelligence the validation process is vital.

28. Human intelligence reports are usually available only at second-hand (for example, when the original informant talks to a case officer[4] who interprets—often literally—his words to construct an intelligence report), and maybe third- or fourth-hand (the original informant talks to a friend, who more or less indirectly talks to a case officer). Documentary or other physical evidence is often more compelling than the best oral reports[5], and has the advantage of being more accessible to specialised examination, but is usually more difficult to acquire. Conventional oral reporting can be difficult

[2] The term 'Masint' (Measurement and Signature Intelligence) has been coined for at least some of these techniques, though they lack the unifying themes which characterise Sigint and Humint.

[3] Such bodies often also have a wider operational role in the implementation of treaties or Security Council Resolutions.

[4] An official responsible for handling and receiving reports from human intelligence sources.

[5] Such evidence is no more immune to deception or fabrication than is oral testimony, though of a different type.

enough if all in the chain understand the subject under discussion. When the topic is unfamiliar to one or more of the people involved, as can be the case when details of (say) nuclear weapons design are at issue, there is always the chance of misunderstanding. There is in such cases a considerable load on the case officer to be familiar with the subject-matter and sufficiently expert in explaining it. It need only be added that often those involved in providing intelligence may for one reason or another have deliberately mis-represented (or at least concealed) their true identities, their country of origin or their employment to their interlocutors[6], to show how great is the need for careful evaluation of the validity of any information which eventually arrives.

29. The validation of a reporting chain requires both care and time, and can generally only be conducted by the agency responsible for collection. The process is informed by the operational side of the agency, but must include a separate auditing element, which can consider cases objectively and quite apart from their apparent intelligence value. Has the informant been properly quoted, all the way along the chain? Does he have credible access to the facts he claims to know? Does he have the right knowledge to understand what he claims to be reporting? Could he be under opposition control, or be being fed information? Is he fabricating? Can the *bona fides*, activities, movements or locations attributed to those involved in acquiring or transmitting a report be checked? Do we understand the motivations of those involved, their private agenda[7], and hence the way in which their reports may be influenced by a desire to please or impress? How powerful is a wish for (in particular) financial reward? What, if any, distorting effect might such factors exert? Is there—at any stage—a deliberate intention to deceive? Generally speaking, the extent and depth of validation required will depend on the counter-intelligence sophistication of the target, although the complexity of the operational situation will affect the possibility of confusion, misrepresentation or deception.

1.4 ANALYSIS

30. The validation process will often have involved consideration of the coherence and consistency of intelligence being provided by an informant, as one of the ways in which that source's reliability can be tested. But at the next stage, analysis, the factual material inside the intelligence report is examined in its own right. This stage may not be required where the material is self-explanatory, or it may be readily subsumed into assessment and conducted by the same people. But much intelligence is fragmentary or specialised and needs at least a conscious analytic stage. Analysis assembles individual intelligence reports into meaningful strands, whether weapons programmes, military operations or diplomatic policies. Intelligence reports take on meaning as they are put into context. Analysis is also the process required to convert complex technical evidence into descriptions of real-world objects or events.

31. The department which receives the largest quantity of intelligence is the MOD, where analysis is carried out by the DIS[8] whose reports are distributed not only internally in

[6] The ultimate in such deceptions is the classic 'double agent,' who is infiltrated into an espionage network to discover, misinform, expose or pervert it.

[7] We have been assured that SIS has for half a century been viscerally wary of emigre organisations. We return to this below in the context of Iraq.

[8] The DIS also has other management and intelligence collection responsibilities.

the MOD but also to other relevant departments. Although the DIS is a component of the MOD, funded from the Defence Account and managed in accordance with defence priorities, it is a vital component of and contributor to the national intelligence machinery, and its priorities and work programme are linked with those of the Cabinet Office.

32. Analysis can be conducted only by people expert in the subject matter—a severe limitation when the topic is as specialised as biological warfare or uranium enrichment, or the internal dynamics of terrorist cells or networks. A special danger here can be the failure to recognise just what particular expertise is required. The British intelligence assessment of the German V-2 rocket during the Second World War was hindered by the involvement of the main British rocket expert, who opined that the object visible on test-stands could not possibly be a rocket. The unrecognised problem was that he was an expert only on *solid powder* rockets, of the type that the UK had developed for short-range artillery. It was true that a solid firework of the size of the V-2 was, with the technology then available, impracticable. But the Germans had developed *liquid-propellant* rocket engines, with the combustion chamber fed by powerful turbo-pumps. On that subject, there were no British experts.

1.5 ASSESSMENT

33. Assessment may be conducted separately from analysis or as an almost parallel process in the mind of the analyst. Intelligence reports often do not immediately fit into an established pattern, or extend a picture in the expected way. Assessment has to make choices, but in so doing runs the risk of selection that reinforces earlier conclusions. The risk is that uneven standards of proof may be applied; reports that fit the previous model are readily accepted, while contrary reports have to reach a higher threshold. This is not only perfectly understandable, it is the way perception normally operates. But in the intelligence world in which data are scanty, may be deliberately intended to confuse and may sometimes be more inadequate than can be appreciated, normal rules do not apply.
34. In the UK, assessment is usually explicitly described as 'all-source.' Given the imperfections of intelligence, it is vital that every scrap of evidence be examined, from the most secret sources through confidential diplomatic reports to openly published data. Intelligence cannot be checked too often. Corroboration is always important but seldom simple, particularly in the case of intelligence on 'hard targets'[9] such as nuclear, biological or chemical weapons programmes or proliferation networks. The simple fact of having apparently coincident reports from multiple types of intelligence sources is not in itself enough. Although reports from different sources may say the same thing, they may not necessarily *confirm* one another. Is a human intelligence report that a factory has been put into operation confirmed by imagery showing trucks moving around it? Or are both merely based on the same thing—observation of physical external activity? Reporting of different but mutually consistent activities

[9] In a sense, almost all intelligence is conducted against 'hard targets.' If the information were readily available, it would not be necessary to call on intelligence resources to acquire it. But within the hierarchy of intelligence activities it is inevitable, given the protection afforded to nuclear, biological and chemical weapons programmes, that they are among the hardest targets.

can be complementary. This can build up knowledge to produce a picture which is more than the simple sum of the parts. But it may be false, if there is no link between the pieces other than the attractiveness of the resulting picture. Complementary information is not necessarily confirmatory information.

35. Multiple sources may conflict, and common sense has to be used in evaluation. A dozen captured soldiers may have provided mutually consistent and supportive reports about the availability of chemical weapons to their neighbouring battalion. But if these were flatly contradicted by a single report from a senior member of that battalion, which should be believed?
36. It is incorrect to say, as some commentators have done, that 'single source' intelligence is always suspect. A single photograph showing missiles on launchers, supporting a division deployed in the field, trumps any number of agent reports that missiles are not part of a division's order of battle. During the Second World War, innumerable Allied command decisions were taken on the basis of intelligence reports from a single *type* of source (signals intelligence, providing decrypts of high-level German and Japanese military plans and orders), and quite often (e.g. re-routing convoys in the middle of the Atlantic) important decisions had to be taken on the basis of a *single report*. As before, common sense and experience are the key.
37. Assessment must always be aware that there may be a deeper level of reality at which apparently independent sources have a common origin. Multiple sources may have been marshalled in a deception campaign, as the Allies did in Operation Fortitude before D-Day to mislead the German High Command about the location of the landings. Although deception on so grand a scale is rare, the chance of being deceived is in inverse proportion to the number of independent sources—which, for 'hard targets,' are few.
38. Many of the manifestations of nuclear, biological or chemical weapons programmes can have innocuous, or at least non-proscribed, explanations—the 'dual-use' problem. Nuclear developments can be for peaceful purposes. Technologies for the production of chemical and biological agents seldom diverge from those employed in normal civilian chemical or bio-chemical industries. And, in the case of missile development, some procurement and development activities may be permissible.
39. Thus, the recipients of intelligence have normally to make decisions on the basis of the balance of probabilities. That requires, first, the most effective deployment of all possible sources and, secondly, the most objective assessment possible, as unaffected as may be by motives and pressures which may distort judgement.
40. In the UK, central intelligence assessment is the responsibility of the Assessments Staff. This comprises some 30 senior and middle-ranking officials on secondment from other departments, within the Cabinet Office, together with secretarial and administrative support.

1.6 THE JOINT INTELLIGENCE COMMITTEE

41. The agencies and the DIS are brought together with important policy departments in the JIC[10]. The JIC was established in 1936 as a sub-committee of the Committee of

[10] For a fuller description see *National Intelligence Machinery,* HMSO 2001, which puts the JIC into context within the structures of Parliamentary and Cabinet government.

Imperial Defence. During the Second World War, it comprised the heads of the agencies and the three Services' Directors of Intelligence, under the chairmanship of a senior member of the Foreign Office and was joined by other relevant departments such as the Ministry of Economic Warfare, responsible for the Special Operations Executive.

42. The JIC has evolved since 1945. It became part of the Cabinet Office rather than of the Chiefs of Staff organisation in 1957. To the original membership of the JIC (intelligence producers, with users from MOD and the FCO) were added the Intelligence Co-ordinator when that post was established in 1968, the Treasury (1968), the Department of Trade and Industry (1997) and the Home Office (2000). Other departments attend when papers of relevance to them are taken. Representatives of the Australian, Canadian and United States intelligence communities also attend as appropriate. In 1993, the post of Chairman of the JIC and that of the Head of the Cabinet Office's Defence and Overseas Secretariat[11] were combined, the two posts remaining so until 1999. From 1992 to 2002, the chairmanship was combined with the post of Intelligence Co-ordinator. A new post of Security and Intelligence Co-ordinator was created in 2002, taking on the responsibilities of the previous Intelligence Co-ordinator together with wider responsibilities in the field of counter-terrorism and crisis management. The holder became a member of the JIC.
43. The JIC's main function[12], on which its regular weekly meetings are centred, is to provide:

Ministers and senior officials with co-ordinated intelligence assessments on a range of issues of immediate and long-term importance to national interests, primarily in the fields of security, defence and foreign affairs.

The Assessments Staff are central to this role, and the Chief of the Assessments Staff is a member of the JIC in his own right. With the assistance of other departments, the Assessments Staff draft the JIC assessments, which are usually debated at Current Intelligence Groups (CIGs) including experts in the subject before being submitted to the JIC. The JIC can itself ask the Assessments Staff to draft an assessment, but the process is usually triggered by a request from a policy department. The forward programme of assessments to be produced is issued three times a year, but is revised and, when necessary, overridden by matters of more immediate concern. The JIC thus brings together in regular meetings the most senior people responsible for intelligence collection, for intelligence assessment and for the use of intelligence in the main departments for which it is collected, in order to construct and issue assessments on the subjects of greatest current concern. The process is robust, and the assessments that result are respected and used at all levels of government.
44. Intelligence is disseminated at various levels and in different forms. The agencies send reports direct to users in departments and military commands; these reports are used by

[11] From 1984 to the end of 1993 the Chairman of the JIC was also the Prime Minister's Foreign Policy Adviser. This title was revived in September 2001 and assumed by the Head of the Defence and Overseas Secretariat.

[12] The JIC also has other responsibilities, for the establishment of intelligence collection priorities and monitoring of agency performance.

civil and military officials in their daily business, and some of them are selected and brought to Ministers' attention. The JIC's co-ordinated intelligence assessments, formally agreed at their weekly meetings, are sent to Ministers and senior officials. In addition the JIC produces Intelligence Updates and Immediate Assessments whenever required, which are sent to a standard distribution throughout government.

45. A feature of JIC assessments is that they contain single statements of position; unlike the practice in the US, there are no minority reports or noted dissents. When the intelligence is unclear or otherwise inadequate and the JIC at the end of its debate is still uncertain, it may report alternative interpretations of the facts before it such as they are; but in such cases all the membership agrees that the interpretations they are proposing are viable alternatives. The JIC does not (and this is borne out by our examination of several hundred JIC assessments in the course of our Review) characterise such alternatives as championed by individual members who disagree with colleagues' points of view. While the JIC has at times been criticised for its choice of language and the subtlety of the linguistic nuances and caveats it applies[13], it has responded that when the intelligence is ambiguous it should not be artificially simplified.

46. In the sometimes lengthy line that leads to the production of the JIC's output, all the components of the system—from collection through analysis and assessment to a well-briefed and educated readership—must function successfully. Problems can arise if the JIC has to make bricks without (enough) straw. Collection agencies may produce too little intelligence, or too much intelligence about the wrong subjects, or the right intelligence but too late to be of value. Although assessments generated under such circumstances may have proper caveats, with attention drawn to important gaps in knowledge and with the dubious steps in an argument clearly identified, they may reach misleading conclusions. Or—which is equally destructive of their purpose—even if they are correct they may be mistrusted. In either case, the reputation of the JIC product is at risk, and the Committee has on occasion refused to issue drafted papers which it has felt are not sufficiently supported by new intelligence or add nothing to the information already publicly available.

1.7 THE LIMITATIONS OF INTELLIGENCE

47. Intelligence merely provides techniques for improving the basis of knowledge. As with other techniques, it can be a dangerous tool if its limitations are not recognised by those who seek to use it.

48. The intelligence processes described above (validation, analysis, assessment) are designed to transform the raw material of intelligence so that it can be assimilated in the same way as other information provided to decision-makers at all levels of government. Validation should remove information which is unreliable (including reporting which has been deliberately inserted to mislead). Analysis should assemble fragmentary intelligence into coherent meaningful accounts. Assessment should put

[13] We have been told that some readers believe that important distinctions are intended between such phrases as "intelligence indicates . . .", "intelligence demonstrates . . ." and "intelligence shows . . .", or between "we assess that . . .", "we judge that . . ." and "we believe that . . .". We have also been told that there is in reality no established glossary, and that drafters and JIC members actually employ their natural language.

intelligence into a sensible real-world context and identify how it can affect policy-making. But there are limitations, some inherent and some practical on the scope of intelligence, which have to be recognised by its ultimate recipients if it is to be used wisely.

49. The most important limitation on intelligence is its incompleteness. Much ingenuity and effort is spent on making secret information difficult to acquire and hard to analyse. Although the intelligence process may overcome such barriers, intelligence seldom acquires the full story. In fact, it is often, when first acquired, sporadic and patchy, and even after analysis may still be at best inferential.
50. The very way that intelligence is presented can contribute to this misperception. The necessary protective security procedures with which intelligence is handled can reinforce a mystique of omniscience. Intelligence is not only—like many other sources—incomplete, it can be incomplete in undetectable ways. There is always pressure, at the assessment stage if not before, to create an internally consistent and intellectually satisfying picture. When intelligence becomes the dominant, or even the only, source of government information, it can become very difficult for the assessment process to establish a context and to recognise that there may be gaps in that picture.
51. A hidden limitation of intelligence is its inability to transform a mystery into a secret. In principle, intelligence can be expected to uncover secrets. The enemy's order of battle may not be known, but it is knowable. The enemy's intentions may not be known, but they too are knowable. But mysteries are essentially unknowable: what a leader *truly* believes, or what his reaction would be in certain circumstances, cannot be known, but can only be judged. JIC judgements have to cover both secrets and mysteries. Judgement must still be informed by the best available information, which often means a contribution from intelligence. But it cannot import certainty.
52. These limitations are best offset by ensuring that the ultimate users of intelligence, the decision-makers at all levels, properly understand its strengths and limitations and have the opportunity to acquire experience in handling it. It is not easy to do this while preserving the security of sensitive sources and methods. But unless intelligence is properly handled at this final stage, all preceding effort and expenditure is wasted.

1.8 RISKS TO GOOD ASSESSMENT

53. It is a well-known phenomenon within intelligence communities that memory of past failures can cause over-estimation next time around. It is equally possible to be misled by past success. For 45 years of Cold War, the intelligence community's major task was to assess the intentions and capabilities of the Soviet Union and its satellite states[14]. As the details which had been sought became more accessible, first through *glasnost'* and explicit exchanges of data under international agreements and then fairly readily through open sources after the dissolution of the Soviet empire, most of the intelligence community's conclusions were vindicated—at least in the areas in

[14] The intelligence community did, of course, have many other tasks during this period ranging from the consequences of the withdrawal from empire through the many facets of the conflicts and confrontations in the Middle East to the Falklands War.

which it had spent the largest part of its efforts, the Soviet bloc's military equipment, capabilities and order of battle.

54. But it is risky to transfer one model to cases where that model will only partially apply. Against dictatorships, dependent upon personal or tribal loyalties and insensitive to international politics, an approach that worked well for a highly-structured, relatively cohesive state target is not necessarily applicable even though many aspects of the work may appear to be identical. The targets which the UK intelligence community needs to study most carefully today are those that structurally and culturally look least like the Government and society it serves. We return to this when we consider terrorism, at Chapter 3.
55. Risks in intelligence assessment will arise if this limitation is not readily recognised. There may be no choice but to apply the same intelligence processes, methods and resources to one target as were developed for and applied to others. But it is important to recognise that the resulting intelligence may need to be analysed and assessed in different ways.
56. A further risk is that of 'mirror-imaging'—the belief that can permeate some intelligence analysts that the practices and values of their own cultures are universal. The more diffuse range of security challenges of the 21st century means that it will not be possible to accumulate the breadth and depth of understanding which intelligence collectors, analysts and users built up over the years about the single subject of the Soviet Union. But the more alien the target, the more important is the ability of intelligence analysts to appreciate that their own assumptions do not necessarily apply everywhere. The motives and methods of non-state organisations built on a special interest (whether criminal, religious or political) can be particularly hard for members of a stable society to assess.
57. There is also the risk of 'group think'—the development of a 'prevailing wisdom.' Well-developed imagination at all stages of the intelligence process is required to overcome preconceptions. There is a case for encouraging it by providing for structured challenge, with established methods and procedures, often described as a 'Devil's advocate' or a 'red teaming' approach. This may also assist in countering another danger: when problems are many and diverse, on any one of them the number of experts can be dangerously small, and individual, possibly idiosyncratic, views may pass unchallenged.
58. One final point should be mentioned here, to which we return in our Conclusions. The assessment process must be informed by an understanding of policy-makers' requirements for information, but must avoid being so captured by policy objectives that it reports the world as policy-makers would wish it to be rather than as it is. The JIC is part (and an important part) of the UK's governmental machinery or it is nothing; but to have any value its product must be objective. The JIC has always been very conscious of this.

1.9 THE USE OF INTELLIGENCE

59. In addition to the use of intelligence to inform government policy, which we describe in Chapters 2 and 3, there are important applications in the enforcement of compliance with national law or international treaties and other obligations, in warning of untoward events, in the support of military and law enforcement operations, and in long-term planning for future national security capabilities. The British Government's machinery for the areas covered by our Review is described at Chapter 4.

CHAPTER 3 TERRORISM[1]

3.1 SCOPE

110. We have examined intelligence reports and assessments on the links between terrorism and chemical, biological, radiological and nuclear weapons, and the use made of that intelligence, from when it began in the early 1990s to emerge as a topic of interest to the Joint Intelligence Committee (JIC). For the purpose of illustrating the contribution made by intelligence to policy formulation by the Government and to actions taken on the basis of that policy, we have focussed on the scope and quality of intelligence reports and assessments on the use by terrorists and extremists of unconventional weapons, and the extent to which they were validated by subsequent discoveries in Afghanistan. To avoid prejudicing current operations, we do not cover in this Report more recent intelligence assessments or findings.

3.2 THE PERIOD UP TO 1995

111. In the late 1980s, the possibility that terrorist groups might seek to use unconventional weapons was considered remote. In surveys of nuclear, biological and chemical weapons proliferation in 1989, the JIC dealt briefly with the possibility that such technology might be used by terrorists:

> *We believe that even the most sophisticated and well-organised terrorist group is highly unlikely to be able to steal and then detonate a nuclear weapon with the foreseeable future. . . . At present the most feasible terrorist nuclear incident would probably be a credible hoax. A terrorist threat to detonate a nuclear device would be difficult to dismiss entirely in view of the increasing number of producers of fissile material in a variety of countries and the problems of accounting fully for all material produced. Terrorists might see a seemingly plausible and preferably well publicized warning of an imminent nuclear attack as potentially a very effective means of blackmailing governments.* [JIC, July 1989]

and:

> *We have no intelligence that any terrorist group makes CBW agents, possesses any such agents or is currently contemplating attacks using CBW agents or other toxic chemicals. The use of CBW agents by terrorists would generate widespread fear and could cause large numbers of casualties. The mere threat of such use could be sufficient to cause panic.*
>
> *A terrorist would need only small quantities of CW agents. The simpler ones could in principle be made by anyone with a knowledge of A-level chemistry using readily obtainable materials. We believe that terrorist organizations could also readily obtain and handle without surmountable difficulty, suitable bacteria, viruses and certain toxins.*
>
> *Although CBW proliferation undoubtedly increases the risk that CBW agents could be stolen by or even supplied to terrorists by state sponsors . . . this prospect must be viewed against a*

[1] This section is limited to intelligence on the use by terrorists of chemical, biological, radiological and nuclear weapons. The large majority of terrorist actions employ conventional armaments and explosives, and are not relevant to this Review.

background where many suitable agents can be manufactured in small quantities using easily available materials. So as far as terrorism is concerned, proliferation (if it comes about) may not necessarily be much affected by the actions of States with the relevant capability. [JIC, 26 June 1989]

112. The main strands in this assessment set the standard for the next few years. There was no credible evidence of terrorist interest in nuclear, biological or chemical weapons; hoaxes and threats might be more disuptive than actual use; terrorists were very unlikely to be able to acquire nuclear devices; and the fact that some states possessed nuclear, biological or chemical weapons was unlikely to affect the risk of their use by terrorists.
113. In April 1992[2], in its first assessment specifically on the threat of attacks by terrorists using chemical, biological, radiological or nuclear weapons, the JIC considered the technical options, but emphasised the difficulties which were thought likely to render such methods unattractive options for terrorist groups:

They may be deterred by the danger to their own members, or by the risk of alienating the public and especially their own supporters. They may also fear that an attack would cause international outrage leading to determined efforts on an international scale to bring them to book. By contrast, conventional weapons are cheaper, easier to procure, and offer equal or greater effectiveness against traditional targets (such as prominent individuals, members of the security forces, government buildings). [JIC, 23 April 1992]

This, too, was to become a feature of JIC assessments; for most terrorist uses, conventional weapons were better.

114. By October 1994, there had been a number of media reports—some correct—of fissile material being available on the black market. In the first of several such studies, the JIC did not consider that these affected its overall assessment:

Despite the possibility which now exists of obtaining fissile material, it is extremely unlikely that a terrorist group could produce even a crude nuclear device; nor is there any evidence that any group has contemplated the use of nuclear weapons. A more plausible scenario might be the dispersal of radioactive materials by conventional explosives or other means to achieve radiological contamination. The actual danger to the public from radioactivity would probably be small—smaller in some cases than to the terrorists. But such an attack (or its threat) could be highly effective in causing panic and public concern.

We believe that terrorists would not be able to acquire or deploy a nuclear weapon; radiological attacks are possible but unlikely. Attacks involving chemical or biological agents are also unlikely, though use of toxic chemical substances (for which there are some limited precedents) remains a possibility. [JIC, 13–19 October 1994]

3.3 1995–1997

115. By June 1995, the JIC was assessing the threat posed by Islamist extremists; the terrorist threat was spreading outside the Middle East. The JIC commented on the use

[2] It was also in 1992 that a Kurdish terrorist group tried to poison the water supply of a Turkish airbase using cyanide.

of suicide tactics, a strand which was subsequently to become significant in such assessments:

Selective interpretation of the Muslim faith enables such groups to justify terrorist violence and to recruit 'martyrs' for suicide attacks. [JIC, 8 June 1995]

116. However, the first serious use of chemicals by terrorists was not by Islamist extremists. The sarin gas attack in the Tokyo underground by the Aum Shinrikyo sect came in March 1995[3]. In a 1996 assessment of the nuclear, biological and chemical threat to the UK[4] (which responded to the G7 declaration at the Lyons summit in June that year that special attention should be paid to the threat of use of nuclear, biological and chemical materials for terrorist purposes) the JIC stuck to its previous line, though noting the Aum Shinrikyo attack:

There is no indication of any terrorist or other group showing interest in the use of nuclear, biological or chemical (NBC) materials against the UK. For a number of reasons, conventional weapons are likely to remain more attractive for terrorist purposes. But last year's nerve agent attack in Tokyo will have heightened interest and, with ever more NBC information publicly available, hoaxes threatening NBC use are likely to become more difficult to assess. [JIC, 4 July 1996]

3.4 1998–1999

117. Usama bin Laden first became known as a high-profile supporter of Islamist extremism while fighting against Soviet forces in Afghanistan during the 1980s. Expelled from Saudi Arabia in 1991 and from Sudan in 1996, he returned to Afghanistan. Evidence of his interest in unconventional weapons accumulated, and was summarised by the JIC in November 1998:

He has a long-standing interest in the potential terrorist use of CBR materials, and recent intelligence suggests his ideas about using toxic materials are maturing and being developed in more detail. . . . There is also secret reporting that he may have obtained some CB material—and that he is interested in nuclear materials. We assess that he lacks the expertise or facilities even to begin making a nuclear weapon, but he might seek to make a radiological device. [JIC, 25 November 1998]

118. Seven months later, in June 1999, the JIC had received more intelligence, and re-assessed the threat from Usama bin Laden's organisation accordingly:

Most of UBL's planned attacks would use conventional terrorist weapons. But he continues to seek chemical, biological, radiological and nuclear material and to develop a capability for its terrorist use. There is insufficient evidence to conclude that he has yet acquired radiological or nuclear material. In contrast, we now assess that his followers have access to some unspecified

[3] The sect had carried out sporadic and unsuccessful open-air attacks using a range of agents since 1990. One attack (using sarin) in Matsumoto in June 1994 caused 7 deaths and 264 people were hospitalised. These earlier attacks were little noticed outside Japan.

[4] Because of its limited ambit this paper did not take note of the then recent Chechen guerrilla operation to place minute quantities of caesium-137 in a Moscow park.

chemical or biological material. Some have received basic training in its use against individuals or in confined spaces.

In April a leading Egyptian terrorist, apparently believing the information was already known to the authorities, told an Egyptian court the UBL had CB 'weapons' which he would use against US or Israeli targets. [JIC, 9 June 1999]

Intelligence reports of bin Laden's associates falling for nuclear materiel frauds suggested, however, that they were not well advised on nuclear matters.

119. A month later, in July 1999, the JIC explained an important change in one of the major assumptions underpinning its previous assessments—some terrorists were no longer reluctant to cause mass casualties, for example some Islamist extremist terrorists and Aum Shinrikyo:

Over the 1990s there has been significant increase in the quantity and quality of intelligence that some terrorists are interested in CBRN—and particularly in chemical and biological—materials as weapons. The risk of a CBRN terrorist incident has risen, albeit from a low base. In part this increase reflects the rise of Islamic extremism and ethnic hatred as terrorist motivations: some of the terrorists thus motivated are less constrained by considerations such as public support, casualties among innocent bystanders, or the prospect of retaliation. It may also reflect the increasing availability of information about making and using CB materials, and t he publicity attracted by major incidents and hoaxes. Whether the attacker's aim is political or economic blackmail, or severe disruption, society's vulnerability to terrorist attack from CB or radiological materials is high, exacerbated by the lack of a tried and tested CB counter-terrorist response in some countries. [JIC, 15 July 1999]

120. In the same assessment, the JIC made its own judgement, in the absence of specific intelligence, that Usama bin Laden had after several years been successful in acquiring non-conventional weapons. That judgement was later shown to be correct:

There have been important developments in [Islamist extremist] *terrorism. It has become clear that Usama Bin Laden has been seeking CBRN materials . . . His wealth permits him to fund procurement, training and experimentation to an extent unmatched by other terrorists. . . . Given the quality and quantity of intelligence about his interest in CB materials, the length of time he has sought them, and the relative ease with which they can be made, we assess that he has by now acquired or made at least modest quantities of CB materials—even if their exact nature and effectiveness are unclear. The significance of his possession of CB materials is that, in contrast to other terrorists interested in CB, he wishes to target US, British and other interests worldwide. There is also intelligence on training in the use of chemicals as weapons in a terrorist camp in Afghanistan, although it is not yet clear if this is under Bin Laden's auspices. The CB threat is likely to be higher abroad than in the UK, reflecting the location of Bin Laden and his allies, the vulnerability of potential targets, and the effectiveness of local security authorities. Targets may include British official sites or related facilities overseas. That said, Bin Laden's attacks remain more likely to employ conventional weapons than CB materials.* [JIC, 15 July 1999]

121. However the JIC still retained its overall conclusion, that:

. . . the indications of terrorist interest in CBRN materials have yet to be matched by a comparable amount of evidence about possession and intent to use CBRN. Most terrorists continue to favour

conventional weapons, as easier to use, more reliable, safer and more controllable than CBRN materials. [JIC, 15 July 1999]

3.5 2000–2001

122. By January 2000, in an assessment of conventional threats, the JIC summarised bin Laden's aspirations for non-conventional weapons:

UBL retains his interest in obtaining chemical, biological, radiological and nuclear (CBRN) materials and expertise. In autumn 1999 there was intelligence that he had recruited . . . chemicals specialists. . . . Our assessment remains that UBL has some toxic chemical or biological materials, and an understanding of their utility as terrorist weapons. But we have yet to see hard intelligence that he possesses genuine nuclear material. [JIC, 12 January 2000]

123. By August 2000, the JIC was clear that, although there were other Islamist extremist groups[5] with an interest in non-conventional weapons, Usama bin Laden posed the most severe threat:

Some [Islamist extremist groups] *are interested in exploring the use of chemical or biological materials as weapons. In the forefront is UBL . . .* [JIC, 9 August 2000]

124. In January 2001, the JIC reported at length on the terrorist threat from unconventional weapons and emphasised the unique nature of the threat from Usama bin Laden:

The actual threat does not match the media hype. Almost all the available intelligence refers to terrorist interest in CB materials, rather than to specific attack plans. There is no credible intelligence that any terrorist except UBL has the capability or serious intent to explore the use of weapons-grade nuclear materials—nor, except for Chechen extremists, radiological material. Terrorists interested in CB are generally those least constrained by public opinion or their members' or supporters' sensitivities. Their resources and targets tend to be abroad rather than in Britain, so the risk of attacks using toxic materials has always been greater overseas.

UBL has sought CBRN materials for use as terrorist weapons. . . . From his public statements and interviews it is clear that he believes it is legitimate to use them as weapons and his wealth has allowed him to fund procurement, experimentation and training. There is plentiful intelligence that this interest is sustained, mostly relating to toxic materials.

In 1999 he sought equipment for a chemical weapons lab in Afghanistan, and claimed already to have . . . experts working there. [JIC, 10 January 2001]

3.6 THE AFTERMATH OF 9/11

125. In an important paper shortly after the attacks of 11 September 2001, the JIC made clear the way in which Usama bin Laden's philosophy, combined with suicide attacks, had changed the calculus of threat. This assessment summarised the new security

[5] The JIC was a year later to comment that the word 'groups' can be misleading in the context of Islamist extremist terrorists. "*There are established groups in different countries, usually working to a national agenda, but the networks associated with UBL are changeable ad hoc groupings of individuals who share his agenda, and who may come together only for a particular operation. Nevertheless, 'groups' is used as a short form for want of another available term.*"

challenge which, as we describe further in the context of Iraq at Chapter 5, was to become dominant in the thinking of British Ministers—the desire of terrorists and extremists to cause casualties on a massive scale, undeterred by the fear of alienating the public or their own supporters that had been noted as a constraining factor in JIC assessments in the early 1990s or by considerations of personal survival. To this fundamental shift in the JIC's judgement on the likely motivation and goals of terrorists and extremists was added a corresponding shift in its conclusions about the attractiveness of nuclear, biological or chemical weapons. Thus, in September 2001 the JIC noted that:

Many defensive and preventive measures taken against terrorism (such as ensuring that passenger and luggage travel together) still presuppose that the terrorist will want to survive the attack. But suicide attackers, especially those backed by sophisticated planning and pursuing non-negotiable objectives, negate many security measures and widen society's vulnerability. New strategies are required to counter the threat of terrorists willing, or even eager, to sacrifice their lives as martyrs in Islamic extremist or other causes—although there can be no complete protection against them.

In the context of UBL's jihad, casualties and destruction could be an end in themselves as much as a means to an end (Footnote: UBL's stated objective is to secure US withdrawal from the Middle East or, failing that, to provoke a reaction which would further demonise the US in the eyes of Muslims and destabilise moderate Arab states that he perceives as un-Islamic). He has no interest in negotiation and there is no indication that he can be deterred. [JIC, 18 September 2001]

126. The JIC also went on in this paper to note Usama bin Laden's interest in nuclear devices.

127. The British Government's dossier of 4 October 2001[6], which attributed the attacks of 11 September 2001 to Usama bin Laden, also reflected the attractiveness to him of nuclear, biological and chemical weapons, saying that:

From the early 1990s Usama bin Laden has sought to obtain nuclear and chemical materials for use as weapons of terror.

and reminding its readership that:

When asked in 1998 about obtaining chemical or nuclear weapons he said "acquiring such weapons for the defence of Muslims (was) a religious duty". [Government's dosssier, 4 October 2001]

3.7 INTELLIGENCE ON UBL'S CAPABILITIES AND ITS VALIDATION

128. A considerable quantity of evidence of Usama bin Laden's capabilities in the nuclear, biological and chemical fields was uncovered after the US-led military action in Afghanistan in October 2001. This section compares these discoveries with JIC judgements beforehand.

[6] "Responsibility for the Terrorist Atrocities in the United States, 11 September 2001".

NUCLEAR

129. In 1999, the JIC reported Usama bin Laden's claims to be setting up a laboratory in Afghanistan. Following the collapse of the Taliban regime, in January 2002 the United Nations Security Council listed a former Pakistani nuclear scientist Bashir Mahmoud as associated with the Taliban or Al Qaida.

CHEMICAL

130. Intelligence reporting from 1999 onwards testified to the activities of Abu Khabbab, an explosives and chemicals expert who ran training courses which included information on how to make and use poisons. This was confirmed by discoveries in Afghanistan such as a video showing chemical experiments being carried out on animals, and by the finding of numerous training manuals.

BIOLOGICAL

131. In 1999, the JIC reported that:

> *In February 1999 one of his followers claimed that UBL intended to attack US and UK targets in India, Indonesia and the US, by using means which even the US could not counter, implying the use of chemical or biological material.* [JIC, 9 June 1999]

132. Some work with biological agents was also attributed to Abu Khabbab, though the evidence was not detailed. However, the JIC's judgement that Al Qaida was developing biological weapons was confirmed by the discovery in Afghanistan of the Kandahar laboratory, and evidence that scientists had been recruited.

3.8 INTELLIGENCE RESPONSES TO INTERNATIONAL TERRORISM

133. Few of the measures being taken by the Government to improve the response to the terrorist threat are unique to attacks using chemical, biological, radiological and nuclear materials. The threat is international, and has motivated intelligence organisations to intensify both national and international collaboration on an unprecedented scale. **All of the UK intelligence agencies are developing new techniques, and we have seen clear evidence that they are co-operating at all levels.**
134. The most obvious embodiment of enhanced inter-departmental co-operation in the UK is the Joint Terrorism Analysis Centre (JTAC). This is a multi-agency organisation, hosted by the Security Service but staffed by personnel seconded from all of the agencies, law enforcement organisations and relevant departments. Its staff retain links to their parent departments and, operating on a round-the-clock basis, pool information to produce continuous assessments of threats within the UK, to British interests abroad and of terrorist activities generally. **JTAC has now been operating for over a year and has proved a success.**
135. The Security Service and Home Office are improving public education, through web sites and by other means, for both long-term and immediate appreciation of terrorist threats.

136. **International counter-terrorism collaboration has also been significantly enhanced in the past six or seven years. Though we understand that other countries have not yet achieved the same level of inter-departmental synthesis, considerable developments have taken place. Staff of the UK intelligence and security agencies are today in much wider contact with their opposite numbers throughout the world.** We have, for example, been briefed on a recent successful counter-terrorist operation which involved eight different countries working together. **We note these initiatives, but remain concerned that the procedures of the international community are still not sufficiently aligned to match the threat.**

GLOSSARY

ACCM	Alternative or Compensatory Control Measure
AFIO	Association of Former Intelligence Officers
AG	Attorney General
Aman	Agaf ha-Modi'in (Israeli military intelligence)
ANC	African National Congress
BDA	Battle Damage Assessment
BfV	Bundesamt für Verfassungsschutz (German equivalent of the FBI)
BMD	Ballistic Missile Defense
BND	Bundesnachrichtendienst (German foreign intelligence service)
BSO	Black September Organization
BW	Biological Weapons
CA	Covert Action
CAS	Covert Action Staff (CIA)
CBW	Chemical/Biological Warfare
CCP	Consolidated Cryptographic Program
CDA	Congressionally Directed Action
CE	Counterespionage
CHAOS	Code name for CIA illegal domestic spying
CI	Counterintelligence
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CIG	Central Intelligence Group
CMS	Community Management Staff
CNC	Crime and Narcotics Center (CIA)

COINTELPRO	FBI Counterintelligence Program
COMINT	Communications Intelligence
Corona	Codename for first U.S. spy satellite system
COS	Chief of Station (CIA)
COSPO	Community Open Source Program Office
CPA	Covert Political Action
CPSU	Communist Party of the Soviet Union
CSI	Committee on Intelligence Services (Britain)
CT	Counterterrorism
CTC	Counterterrorism Center (CIA)
CW	Chemical Weapons
D & D	Denial and Deception
DARP	Defense Airborne Reconnaissance Program
DAS	Deputy Assistant Secretary
DBA	Dominant Battlefield Awareness
DC	Deputies Committee (NSC)
DCD	Domestic Contact Division (CIA)
DCI	Director of Central Intelligence
D/CIA	Director of Central Intelligence Agency
DDA	Deputy Director of Administration (CIA)
DDCI	Deputy Director for Central Intelligence (DDCI)
DD/CIA	Deputy Director, Central Intelligence Agency
DDO	Deputy Director for Operations (CIA)
DDP	Deputy Director for Plans (CIA)
DDS&T	Deputy Director for Science and Technology (CIA)
DEA	Drug Enforcement Administration
DGSE	Directorie Génerale de la Sécurité Extérieure (French intelligence service)
DHS	Department of Homeland Security
DI	Directorate of Intelligence (CIA)
DIA	Defense Intelligence Agency
DIA/Humint	Defense Humint Service
DINSUM	*Defense Intelligence Summary*
DNI	Director of National Intelligence
DO	Directorate of Operations
DoD	Department of Defense
DOD	Domestic Operations Division (CIA)
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Treasury
DOS	Department of State
DP	Directorate of Plans (CIA)
DST	Directoire de Surveillance Territore (France)
ECHR	European Convention of Human Rights

ELINT	Electronic Intelligence
ENIGMA	Code machine used by the Germans during World War II
EO	Executive Order
EOP	Executive Office of the President
ETF	Environmental Task Force (CIA)
FARC	Fuerzas Armadas Revolucionarias in Colombia
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FISA	Foreign Intelligence Surveillance Act (1978)
FNLA	National Front for the Liberation of Angola
FOIA	Freedom of Information Act
FRD	Foreign Resources Division (CIA)
FSB	Federal'naya Sluzba Besnopasnoti (Federal Security Service, Russia)
GAO	General Accountability Office (Congress)
GCHQ	Government Communications Headquarters (the British NSA)
GEO	Geosynchronous Orbit
GEOINT	Geospatial Intelligence
GRU	Soviet Military Intelligence
GSG	German Counterterrorism Service
HEO	High Elliptical Orbit
HPSCI	House Permanent Select Committee on Intelligence
HUAC	House Un-American Activities Committee
HUMINT	Human Intelligence (assets)
I & W	Indicators and Warning
IAEA	International Atomic Energy Agency
IAF	Israel Air Force
IC	Intelligence Community
ICS	Intelligence Community Staff
IDF	Israeli Defense Force
IG	Inspector General
IMINT	Imagery Intelligence (photographs)
INR	Bureau of Intelligence and Research (Department of State)
INTELINK	An intelligence community computer information system
INTs	Collection disciplines (IMINT, SIGINT, OSINT, HUMINT, MASINT)
IOB	Intelligence Oversight Board (White House)
ISA	Israeli Security Agency
ISC	Intelligence and Security Committee (U.K.)
ISI	Inter-Services Intelligence (Pakistani intelligence agency)
IT	Information Technology
JCAE	Joint Committee on Atomic Energy
JCS	Joint Chiefs of Staff
JIC	Joint Intelligence Committee (U.K.)

JSOC	Joint Special Operations Command
JSTARS	Joint Surveillance Target Attack Radar Systems
KGB	Soviet Secret Police
KH	Keyhole (satellite)
LTTE	Tamil Tigers of Tamil Elam
MAGIC	Allied code-breaking operations against the Japanese in the World War II
MASINT	Measurement and Signatures Intelligence
MI5	Security Service (U.K.)
MI6	Secret Intelligence Service (U.K.)
MON	Memoranda of Notification
MONGOOSE	Code name for CIA covert actions against Fidel Castro of Cuba (1961–62)
Mossad	Israeli Intelligence Service
MPLA	Popular Movement for the Liberation of Angola
NAACP	National Association for the Advancement of Colored People
NBC	Nuclear, Biological, and Chemical (Weapons)
NCS	National Clandestine Service
NCIC	National Counterintelligence Center
NCTC	National Counterterrorism Center
NED	National Endowment for Democracy
NFIB	National Foreign Intelligence Board
NFIC	National Foreign Intelligence Council
NFIP	National Foreign Intelligence Program
NGA	National Geospatial-Intelligence Agency
NGO	Nongovernmental organization
NIA	National Intelligence Authority
NIC	National Intelligence Council
NID	*National Intelligence Daily*
NIE	National Intelligence Estimate
NIO	National Intelligence Officer
NOC	Nonofficial Cover
NPIC	National Photographic Interpretation Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council (White House)
NSCID	National Security Council Intelligence Directive
NTM	National Technical Means
OB	Order of Battle
OC	Official Cover
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
ONI	Office of Naval Intelligence

OPC	Office of Policy Coordination
OSD	Office of the Secretary of Defense
OSINT	Open-Source Intelligence
OSS	Office of Strategic Services
P & E	Processing and Exploitation
PDB	*President's Daily Brief*
PFIAB	President's Foreign Intelligence Advisory Board (White House)
PFLP	Popular Front for the Liberation of Palestine
PIJ	Palestinian Islamic Jihad
PLO	Palestine Liberation Organization
PM	Paramilitary
PRO	Public Record Office (U.K.)
RADINT	Radar Intelligence
RFE	Radio Free Europe
RL	Radio Liberty
SA	Special Activities Division (DO/CIA)
SAS	Special Air Service (U.K.)
SBS	Special Boat Service (U.K.)
SDO	Support to Diplomatic Operations
SHAMROCK	Code name for illegal NSA interception of cables
SIG	Senior Interagency Group
SIGINT	Signals Intelligence
SIS	Secret Intelligence Service (U.K., also known as MI6)
SISDE	Italian Intelligence Service
SMO	Support to Military Operations
SMS	Secretary's *Morning Summary* (Department of State)
SNIE	Special National Intelligence Estimate
SO	Special Operations (CIA)
SOCOM	Special Operations Command (Department of Defense)
SOE	Special Operations Executive (U.K.)
SOG	Special Operations Group (DO/CIA)
SOVA	Office of Soviet Analysis (CIA)
SSCI	Senate Select Committee on Intelligence
SVR	Russian Foreign Intelligence Service
TECHINT	Technical Intelligence
TELINT	Telemetery Intelligence
TIARA	Tactical Intelligence and Related Activities
TPED	Tasking, Processing, Exploitation, and Dissemination
UAV	Unmanned Aerial Vehicle (drone)
ULTRA	Code name for the Allied operation that deciphered the German ENIGMA code in World War II
UN	United Nations
UNITA	National Union for the Total Independence of Angola

UNSCOM	United Nations Special Commission
USIB	United States Intelligence Board
USTR	United States Trade Representative
VCI	Viet Cong Infrastructure
VENONA	Code name for SIGINT intercepts against Soviet spying in America
VOA	Voice of America
VX	A deadly nerve agent used in chemical weapons
WMD	Weapons of mass destruction

INDEX

ABOUT THE EDITOR AND CONTRIBUTORS

EDITOR

Loch K. Johnson is Regents Professor of Public and International Affairs at the University of Georgia and author of several books and over 100 articles on U.S. intelligence and national security. His books include *The Making of International Agreements* (1984); *A Season of Inquiry* (1985); *Through the Straits of Armageddon* (1987, coedited with Paul Diehl); *Decisions of the Highest Order* (1988, coedited with Karl F. Inderfurth); *America's Secret Power* (1989); *Runoff Elections in the United States* (1993, coauthored with Charles S. Bullock III); *America as a World Power* (1995); *Secret Agencies* (1996); *Bombs, Bugs, Drugs, and Thugs* (2000); *Fateful Decisions* (2004, coedited with Karl F. Inderfurth); *Strategic Intelligence* (2004, coedited with James J. Wirtz); *Who's Watching the Spies?* (2005, coauthored with Hans Born and Ian Leigh); *American Foreign Policy* (2005, coauthored with Daniel Papp and John Endicott); and *Seven Sins of American Foreign* Policy (2007). He has served as special assistant to the chair of the Senate Select Committee on Intelligence (1975–76), staff director of the House Subcommittee on Intelligence Oversight (1977–79), and special assistant to the chair of the Aspin-Brown Commission on Intelligence (1995–96). In 1969–70, he was an American Political Science Association Congressional Fellow. He has served as secretary of the American Political Science Association and President of the International Studies Association, South. Born in New Zealand and educated at the University of California, Johnson has taught at the University of Georgia since 1979, winning its Meigs Professorship for meritorious teaching and its Owens Award for outstanding accomplishments in the field of social science research. In 2000, he led the founding of the School of Public and

International Affairs at the University of Georgia. He is the senior editor of the international journal *Intelligence and National Security*.

CONTRIBUTORS

Matthew M. Aid is Managing Director in the Washington, DC, office of Citigate Global Intelligence and Security and coeditor of *Secrets of Signals Intelligence During the Cold War and Beyond* (2001).

James E. Baker sits on the U.S. Court of Appeals for the Armed Forces. He previously served as Special Assistant to the President and Legal Adviser to the National Security Council and as Deputy Legal Adviser to the NSC. He has also served as Counsel to the President's Foreign Intelligence Advisory Board, an attorney at the Department of State, a legislative aide to Senator Daniel Patrick Moynihan, and as a Marine Corps infantry officer. He is the coauthor with Michael Reisman of *Regulating Covert Action* (Yale University Press, 1992).

David M. Barrett is Associate Professor of Political Science at Villanova University and author of *Congress and the CIA* (Kansas, 2005).

Hans Born is a senior fellow in democratic governance of the security sector at the Geneva Centre for Democratic Control of the Armed Forces (DCAF). He is an external member of the crisis management and security policy faculty of the Federal Institute of Technology and a guest lecturer on governing nuclear weapons at the UN Disarmament Fellowship Programme. He has written, co-authored, and co-edited various books on international relations and security policy, including the Inter-Parliamentary Union Handbook on *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices* (Geneva: IPU/DCAF, 2003, translated in 30 languages); *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005, translated in 10 languages); *Who is Watching the Spies? Establishing Intelligence Agency Accountability* (Dulles, VA: Potomac Publishers, 2005); *Civil-Military Relations in Europe: Learning from Crisis and Institutional Change* (London: Routledge, 2006); and *The Double Democratic Deficit: Parliamentary Accountability and the Use of Force under International Auspices* (London: Ashgate Publishers: Aldershot).

A. Denis Clift is President of the Department of Defense Joint Military Intelligence College. He was born in New York City and educated at Friends Seminary, Phillips Exeter Academy (1954), Stanford University (B.A., 1958), and the London School of Economics and Political Science (M.Sc., 1967). He began a career of public service as a naval officer in the Eisenhower and Kennedy administrations and has served in military and civilian capacities in ten administrations, including thirteen successive years in the Executive Office of the President and the White House. From 1971–76, he served on the National Security

Council staff. From 1974–76, he was head of President Ford's National Security Council staff for the Soviet Union and Eastern and Western Europe. From 1977–81, he was Assistant for National Security Affairs to the Vice President. From 1991–94, he was Chief of Staff, Defense Intelligence Agency. From 1963–66, he was the editor of the U.S. Naval Institute *Proceedings*. His published fiction and nonfiction include the novel *A Death in Geneva* (Ballantine Books, Random House), *Our World in Antarctica* (Rand McNally), *With Presidents to the Summit* (George Mason University Press), and *Clift Notes: Intelligence and the Nation's Security* (JMIC Writing Center Press).

William J. Daugherty holds a doctorate in government from the Claremont Graduate School and is Associate Professor of government at Armstrong Atlantic State University in Savannah, Georgia. A retired senior officer in the CIA, he is also the author of *In the Shadow of the Ayatollah: A CIA Hostage in Iran* (Annapolis, 2001) and *Executive Secrets: Covert Action and the Presidency* (Kentucky, 2004).

Jack Davis served in the CIA from 1956 to 1990 as analyst, manager, and teacher of analysts. He now is an independent contractor with the Agency, specializing in analytic methodology. He is a frequent contributor to the journal *Studies in Intelligence*.

Stuart Farson is Lecturer, Political Science Department, Simon Fraser University, Vancouver/Surrey, Canada. He is a former Secretary-Treasurer of the Canadian Association for Security and Intelligence Studies, and served as Director of Research for the Special Committee of the House Commons (Canada) on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act. He has numerous articles on security, intelligence, and policing issues and is the coeditor of *Security and Intelligence in a Changing World* (with David Stafford and Wesley K. Wark, Cass, 1991).

Timothy Gibbs is a final-year doctoral student in history at Robinson College, Cambridge University, and a member of the Cambridge University Intelligence Seminar. He is also a former Visiting Scholar at the University of Georgia. His doctoral dissertation, titled *British and American Intelligence and the Atom Spies*, was submitted in the summer of 2006 and was supervised by Professor Christopher Andrew.

Peter Gill is Reader in Politics and Security, Liverpool John Moores University, Liverpool, United Kingdom. He is coauthor of *Introduction to Politics* (1988, 2nd ed.) and *Intelligence in an Insecure World* (2006). He is currently researching the control and oversight of domestic security in intelligence agencies.

Harold M. Greenberg graduated with a B.A. in history from Yale University in 2005. At Yale, he participated in the Studies in Grand Strategy program, and he has recently published research on CIA covert action in the 1950s. He now works as a legislative aide in the U.S. House of Representatives.

Daniel S. Gressang IV is Professor at the Joint Military Intelligence College (JMIC) in Washington, DC, and serves concurrently as the National Security Agency/National Cryptologic School of Liaison to JMIC. He has researched, written, and lectured extensively on terrorism and counterinsurgency. His research focuses primarily on the application of complex adaptive systems perspectives to understanding the dynamics of terror and other forms of unconventional warfare. In 2004, he was designated Intelligence Community Officer by the Director of Central Intelligence.

Glenn Hastedt received his doctorate in political science from Indiana University. Until recently he was Professor and Chair of the Political Science Department at James Madison University. He is now chair of the Justice Studies Department there. Among his publications is *American Foreign Policy: Past, Present, Future*, 6th ed. (Prentice Hall).

John Hollister Hedley, during more than thirty years at CIA, edited the *President's Daily Brief*, briefed the *PDB* at the White House, served as Managing Editor of the *National Intelligence Daily*, and was Chairman of the CIA's Publications Review Board. Now retired, Hedley has taught intelligence at Georgetown University and serves as a consultant to the National Intelligence Council and the Center for the Study of Intelligence.

Michael Herman served from 1952 to 1987 in Britain's Government Communications Headquarters, with secondments to the Cabinet Office and the Ministry of Defence. Since retirement he has written extensively on intelligence matters, with official clearance. He has had academic affiliations with Nuffield and St. Antony's Colleges in Oxford and is Founder Director of the Oxford Intelligence Group and Honorary Departmental Fellow at Aberystwyth University. In 2005 he received the degree of Honorary D.Litt from Nottingham University. He is a leading British intelligence scholar and author of *Intelligence Power in Peace and War* (Cambridge, 2001).

Frederick P. Hitz is Lecturer (Diplomat in Residence) in Public and International Affairs, Woodrow Wilson School, Princeton University.

Max M. Holland is the author of *The Kennedy Assassination Tapes* (Knopf, 2004).

Arthur S. Hulnick is Associate Professor of International Relations at Boston University. He is a veteran of thirty-five years of intelligence service, including seven years in Air Force Intelligence and twenty-eight years in the CIA. He is author of *Fixing the Spy Machine* (Praeger, 1999) and *Keeping Us Safe* (Praeger, 2004).

Rhodri Jeffreys-Jones is Professor of American History at the University of Edinburgh. The author of several books on intelligence history, he is currently completing a study of the FBI.

Ephraim Kahana is Professor of Political Science and faculty member in the Western Galilee College, Acre, Israel. He teaches courses on international relations, national security and intelligence, and foreign policy in the National Security Program in the University of Haifa. Kahana has written numerous papers on intelligence and foreign policy. His most recent book is the *Historical Dictionary of Israeli Intelligence* (2006).

Patrick Radden Keefe is a graduate of the School of Law at Yale University and is presently a Fellow with the Century Foundation in New York City. He is the author of *Chatter: Uncovering the Echelon Surveillance Network and the Secret World of Global Eavesdropping* (Random House, 2006), and has published essays in *The New York Review of Books*, *The New York Times Magazine*, the *New York Times*, the *Boston Globe*, the *Yale Journal of International Law*, *Legal Affairs*, *Slate*, and *Wired*. He has been a Marshall Scholar and a 2003 fellow at the Dorothy and Lewis B. Cullman Center for Scholars and Writers at the New York Public Library.

Jennifer D. Kibbe is Assistant Professor of Government at Franklin and Marshall College. Between 2002 and 2004, she was a postdoctoral fellow at the Brookings Institution. Her research interests include U.S. foreign policy, intelligence and covert action, presidential decision making, and political psychology. She has published work on U.S. policy in Iraq and the Middle East, and the military's involvement in covert actions.

Katharina von Knop is a doctoral candidate in Political Science at Leopold-Franzens University in Innsbruck, Austria, specializing in counter- and antiterrorism, and coeditor with Heinrich Neisser and Martin van Creveld of *Countering Modern Terrorism: History, Current Issues, and Future Threats* (2005).

Lawrence J. Lamanna is a doctoral candidate in the School of Public and International Affairs at the University of Georgia. He holds an M.A. from Yale University and a B.A. from the University of Notre Dame.

Ian Leigh is Professor of Law and Codirector of the Human Rights Centre at the University of Durham. He lives in Durham, England.

Kristin M. Lord is Associate Dean at George Washington University's Elliott School of International Affairs. In 2005–2006, she was a Council on Foreign Relations International Affairs Fellow and Special Adviser to the Under Secretary of State for Democracy and Global Affairs. Lord is the author of *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security Democracy or Peace* (SUNY Press, 2006); coeditor, with Bernard I. Finel, of *Power and Conflict in the Age of Transparency* (Palgrave Macmillan, 2000); and the author of numerous book chapters, articles, and papers on international politics and security. Lord received her doctorate in government from Georgetown University.

Minh A. Luong is Assistant Director of International Security Studies at Yale University, where he teaches in the Department of History. He also serves as adjunct Assistant Professor of Public Policy at the Taubman Center at Brown University.

Cynthia M. Nolan earned a doctorate at American University in the School of International Service, researching intelligence oversight. She is a former officer in the Directorate of Operations in the CIA and has published in the *International Journal of Intelligence and Counterintelligence*.

Kevin A. O'Brien is a former research associate with the Canadian Institute of Strategic Studies and is currently a senior analyst for RAND Europe.

Mark Phythian is Professor of International Security and Director of the History and Governance Research Institute at the University of Wolverhampton, United Kingdom. He is the author of *Intelligence in an Insecure World* (2006, with Peter Gill), *The Politics of British Arms Sales Since 1964* (2000), and *Arming Iraq* (1997), as well as numerous journal articles on intelligence and security issues.

Harry Howe Ransom is Professor Emeritus of Political Science at Vanderbilt University. He has a B.A. from Vanderbilt and an M.A. and Ph.D. from Princeton University. He was a Congressional Fellow of the American Political Science Association and a Fellow of the Woodrow Wilson International Center for Scholars. He taught at Princeton, Vassar College, Michigan State University, Harvard University, and the University of Leeds. His books include *Central Intelligence and National Security* (1958), *Can American Democracy Survive Cold War?* (1963), and *The Intelligence Establishment* (1970).

Jeffrey T. Richelson is Senior Fellow with the National Security Archive in Washington, DC, and author of *The Wizards of Langley*, *The U.S. Intelligence Community*, *A Century of Spies*, and *America's Eyes in Space*, as well as numerous articles on intelligence activities. He received his doctorate in political science from the University of Rochester and has taught at the University of Texas, Austin, and the American University, Washington, DC. He lives in Los Angeles.

Jerel A. Rosati is Professor of Political Science and International Studies at the University of South Carolina since 1982. His area of specialization is the theory and practice of foreign policy, focusing on the U.S. policy-making process, decision-making theory, and the political psychological study of human cognition. He is the author and editor of five books and over forty articles and chapters. He has received numerous outstanding teaching awards. He has been Visiting Professor at Somalia National University in Mogadishu and Visiting Scholar at China's Foreign Affairs College in Beijing. He also has been a Research Associate in the Foreign Affairs and National Defense Division of the Library of Congress's Congressional Research Service, President of the International

Studies Association's Foreign Policy Analysis Section, and President of the Southern region of the International Studies Association.

Richard L. Russell is Professor of national security studies at the National Defense University. He is also an adjunct associate professor in the Security Studies Program and research associate in the Institute for the Study of Diplomacy at Georgetown University. He previously served as a CIA political-military analyst. Russell is the author of *Weapons Proliferation and War in the Greater Middle East: Strategic Contest* (2005).

Frederick A. O. Schwarz Jr. received an A.B. from Harvard University and J.D. from Harvard Law School, where he was an editor of the *Law Review*. After a year's clerkship with Hon. J. Edward Lumbard, U.S. Court of Appeals for the Second Circuit, he worked one year for the Nigerian government as Assistant Commissioner for Law Revision under a Ford Foundation grant. He joined the New York City law firm of Cravath, Swaine and Moore in 1963 and was elected a partner in 1969. From 1975 through mid-1976, he served as Chief Counsel to the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the Church Committee); from 1982–89, he served as Corporation Counsel and head of the Law Department of the City of New York. In 1989, he chaired the New York City Charter Revision Commission.

James M. Scott is Professor and Chair of the Department of Political Science at Oklahoma State University. His areas of specialization include foreign policy analysis and international relations, with particular emphasis on U.S. foreign policy making and the domestic sources of foreign policy. He is author or editor of four books, over forty articles, book chapters, review essays, and other publications. He has been President of the Foreign Policy Analysis section and President of the Midwest region of the International Studies Association, where he has also served as conference organizer for both sections and has been a two-time winner of the Klingberg Award for Outstanding Faculty Paper at the ISA Midwest Annual Meeting. Since 1996, he has received over two dozen awards from students and peers for his outstanding teaching and research, including his institution's highest awards for scholarship in 2000 and 2001. Since 2005, he has been Director of the Democracy and World Politics Summer Research Program, a National Science Foundation Research Experience for Undergraduates.

Len Scott is Professor of International Politics at the University of Wales, Aberystwyth, where he is Director of the Centre for Intelligence and International Security Studies. Among his recent publications are *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows* (2004, coedited with Peter Jackson) and *Planning Armageddon: Britain, the United States and the Command of Nuclear Forces, 1943–1964* (2000, coedited with Stephen Twigge).

Katherine A. S. Sibley is Professor and Chair of the History Department at St. Joseph's University. She is currently working on a biography of Florence Kling

Harding, titled *America's First Feminist First Lady*. Sibley's work will revise the typical portrait of Mrs. Harding as manipulative, unhappy wife, casting new light on her public and private life. In 2004, Sibley published *Red Spies in America: Stolen Secrets and the Dawn of the Cold War* with the University Press of Kansas. She is also the author of *The Cold War* (1998) and *Loans and Legitimacy: The Evolution of Soviet-American Relations, 1919–1933* (1996). Her work has appeared in journals including *American Communist History*, *Peace and Change*, and *Diplomatic History*, and she also serves as book review editor for *Intelligence and National Security*. She is a three-term Commonwealth Speaker for the Pennsylvania Humanities Council.

Jennifer Sims is Director of Intelligence Studies and Visiting Professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service. She also consults for the U.S. government and private sector on homeland security and intelligence related matters. Prior to this, Sims was Research Professor at Johns Hopkins University's Nitze School of Advanced International Studies in Washington, DC (Fall 2001–Summer 2003). She has served as defense and foreign policy adviser to Senator John Danforth (1990–94), a professional staff member of the Senate Select Committee on Intelligence (1991–94), Deputy Assistant Secretary of State for Intelligence Coordination (1994–98), and as the Department of State's first Coordinator for Intelligence Resources and Planning in the office of the Under Secretary for Management. In 1998 Sims was awarded the U.S. Intelligence Community's Distinguished Service Medal. She received her B.A. degree from Oberlin College and her M.A. and Ph.D. in national security studies from Johns Hopkins University in 1978 and 1985, respectively. She is the author of a number of books and articles on intelligence and arms control. The most recent of these include "Foreign Intelligence Liaison: Devils, Deals and Details," *International Journal of Intelligence and Counterintelligence Affairs* (Summer 2006); *Transforming US Intelligence,* coedited with Burton Gerber (Georgetown University Press, 2005); "Transforming U.S. Espionage: A Contrarian's Approach," *Georgetown Journal of International Affairs* (Winter/Spring 2005); "Domestic Factors in Arms Control: The U.S. Case," in Jeffrey A Larson (ed.), *Arms Control: Cooperative Security in a Changing Environment* (Lynne Rienner, 2002); "What Is Intelligence? Information for Decision-Makers," in Roy Godson, Ernest R. May, and Gary Schmitt, *U.S. Intelligence at the Crossroads* (Brassey's, 1995); "The Cambridge Approach Reconsidered," *Daedalus* 120 (Winter 1991); and *Icarus Restrained: An Intellectual History of American Arms Control* (Westview Press, 1990).

Robert David Steele is CEO of OSS.Net, an international open source intelligence provider. As the son of an oilman, a Marine Corps infantry officer, and a clandestine intelligence case officer for the CIA, he has spent over twenty years abroad in Asia and Central and South America. As a civilian intelligence officer he spent three back-to-back tours overseas, including one tour as one of the first officers assigned full-time to terrorism, and three headquarters tours in offensive

counterintelligence, advanced information technology, and satellite program management. He resigned from the CIA in 1988 to be the senior civilian founder of the Marine Corps Intelligence Command. He resigned from the Marines in 1993. He is the author of three works on intelligence, as well as the editor of a book on peacekeeping intelligence. He has earned graduate degrees in international relations and public administration, is a graduate of the Naval War College, and has a certificate in Intelligence Policy. He is also a graduate of the Marine Corps Command and Staff Course and of the CIA's Mid-Career Course 101.

John D. Stempel is Senior Professor of International Relations at the University of Kentucky's Patterson School of Diplomacy and International Commerce, where he was Associate Director (1988–93) and Director (1993–2003). He came to the University of Kentucky following a 24-year career in the U.S. Foreign Service. There he focused on political and economic affairs, with overseas assignments in Africa (Guinea, Burundi, Zambia), Iran, and India, concluding with three years as U.S. Consul General in Madras. His Middle East service (1975–79) in Tehran provided the material for his book *Inside the Iranian Revolution*. His subsequent academic writings have focused on religion and diplomacy, intelligence and diplomacy, and American views of negotiation. His Washington assignments featured duty for both the State and Defense Departments, including a two-year tour as Director of the State Department's Crisis Center. He has taught at George Washington and American Universities, plus two years as Diplomat in Residence at the U.S. Naval Academy, Annapolis. Stemple is a member of the New York Council on Foreign Relations and is listed in *Who's Who in the World* and *Who's Who in America*. He holds an A.B. degree from Princeton University and M.A. and Ph.D. degrees from the University of California at Berkeley.

Stan A. Taylor is an Emeritus Professor of Political Science at Brigham Young University in Provo, Utah. He has taught in England, Wales, and New Zealand and in 2006 was a visiting professor at the University of Otago in Dunedin, New Zealand. He is founder of the David M. Kennedy Center for International Studies at Brigham Young University. He writes frequently on intelligence, national security, and U.S. foreign policy.

Athan Theoharis is Professor of History at Marquette University whose research has focused on government secrecy, Cold War politics, and the history of the FBI. He is the author, coauthor, and editor of eighteen books, including *The FBI and American Democracy* (2004), *Chasing Spies* (2002), *A Culture of Secrecy* (1998), and *The FBI: A Comprehensive Reference Guide* (1998). He has received numerous awards, including the American Bar Association's Gavel Award and selection as a fellow by the Wisconsin Academy of Arts, Sciences, and Letters.

Gregory F. Treverton is senior analyst at the RAND Corporation. Earlier, he directed RAND's Intelligence Policy Center and its International Security and Defense Policy Center, and he is Associate Dean of the Pardee RAND Graduate School. His recent work has examined at terrorism, intelligence, and law

enforcement, with a special interest in new forms of public-private partnership. He has served in government for the first Senate Select Committee on Intelligence, handling Europe for the National Security Council, and most recently as vice chair of the National Intelligence Council, overseeing the writing of America's National Intelligence Estimates. He holds an A.B. *summa cum laude* from Princeton University, a master's in public policy, and Ph.D. in economics and politics from Harvard University. His latest books are *Reshaping National Intelligence for an Age of Information* (Cambridge University Press, 2001), and *New Challenges, New Tools for Defense Decisionmaking* (edited, RAND, 2003).

Michael A. Turner is a political scientist who has taught international relations and national security matters in San Diego, California, for the past twelve years. Before that, he spent over fifteen years in various positions within the CIA. Turner is the author of *Why Secret Intelligence Fails* (2005; 2006) and the *Historical Dictionary of United States Intelligence* (2006).

Michael Warner serves as Historian for the Office of the Director of National Intelligence.

Nigel West is a military historian specializing in security and intelligence topics. He is the European editor of the *World Intelligence Review* and is on the faculty at the Center for Counterintelligence and Security Studies in Washington, DC. He is the author of more than two dozen works of nonfiction and recently edited *Guy Liddell Diaries*.

Reg Whitaker is Distinguished Research Professor Emeritus, York University, and Adjunct Professor of Political Science, University of Victoria, Canada. He has written extensively on Canadian and international security and intelligence issues.

James J. Wirtz is Professor in the Department of National Security Affairs at the Naval Postgraduate School, Monterey, California. He is Section Chair of the Intelligence Studies Section of the International Studies Association and President of the International Security and Arms Control Section of the American Political Science Association. Wirtz is the series editor for *Initiatives in Strategic Studies: Issues and Policies*, published by Palgrave Macmillan.

Amy B. Zegart is Associate Professor of Public Policy at the University of California, Los Angeles. A specialist on national and homeland security, she has served on the National Security Council staff, as a foreign policy advisor to the Bush-Cheney 2000 presidential campaign, and as a consultant to California state and local homeland security agencies. She has published articles in leading academic journals, including *International Security* and *Political Science Quarterly*, and is the author of *Flawed by Design: The Origins of the CIA, JCS, and NSC* (Stanford, 1999). She received her Ph.D. in political science from Stanford, where she studied under Condoleezza Rice, and an A.B. in East Asian Studies from Harvard University.

STRATEGIC INTELLIGENCE

STRATEGIC INTELLIGENCE

5

INTELLIGENCE AND ACCOUNTABILITY: SAFEGUARDS AGAINST THE ABUSE OF SECRET POWER

Edited by
Loch K. Johnson

Intelligence and the Quest for Security

PRAEGER SECURITY INTERNATIONAL
Westport, Connecticut • London

Library of Congress Cataloging-in-Publication Data

Strategic intelligence / edited by Loch K. Johnson.
p. cm.—(Intelligence and the quest for security, ISSN 1932-3492)
Includes bibliographical references and index.
ISBN 0-275-98942-9 (set : alk. paper)—ISBN 0-275-98943-7 (vol. 1 : alk. paper)—
ISBN 0-275-98944-5 (vol. 2 : alk. paper)—ISBN 0-275-98945-3 (vol. 3 : alk. paper)—
ISBN 0-275-98946-1 (vol. 4 : alk. paper)—ISBN 0-275-98947-X (vol. 5 : alk. paper)
1. Military intelligence. 2. Intelligence service—Government policy. I. Johnson, Loch K., 1942–

UB250.S6385 2007
327.12—dc22 2006031165

British Library Cataloguing in Publication Data is available.

Library of Congress Catalog Card Number: 2006031165
ISBN: 0-275-98942-9 (set)
0-275-98943-7 (vol. 1)
0-275-98944-5 (vol. 2)
0-275-98945-3 (vol. 3)
0-275-98946-1 (vol. 4)
0-275-98947-X (vol. 5)
ISSN: 1932-3492

First published in 2007

Praeger Security International, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the Untied States of America

The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE

THIS FIVE-VOLUME SERIES IN INTELLIGENCE IS SOMETHING of a landmark in the study of intelligence. Thirty years ago, one would have been hard-pressed to find enough good articles on the subject to fill two volumes, let alone five. In those three decades since 1975, however, the study of intelligence has grown considerably. Today there are several solid professional journals in the field, including the premier publications *Intelligence and National Security* (published in the United Kingdom), *International Journal of Intelligence and Counterintelligence* (the United States), and *Studies in Intelligence* (from the Central Intelligence Agency, in both classified and unclassified form). In just the past two years, bulging anthologies on the general topic "strategic intelligence," as well as a "handbook" on intelligence and a collection of chapters within the more specialized niche of "intelligence and ethics" have appeared, along with a tidal wave of books and articles on one aspect or another of this subject (see the bibliographic essay in volume 1).

Except in times of scandal (Watergate in 1973, CIA domestic spying in 1974, the Iran-*contra* affair in 1987), one could find in this earlier era little newspaper coverage of intelligence activities, so tightly held were these operations by the government. Now, fueled by the events of the September 11, 2001, terrorist attacks and the erroneous prediction in 2002 that weapons of mass destruction (WMDs) were being developed and stockpiled by Iraq, hardly a week goes by without reports on intelligence in the *New York Times* and other leading newspapers. These days, the *Atlantic Monthly* and the *New Yorker*, America's top literary magazines, visit the subject with some regularity, too. The latter has hired Seymour M. Hersh, the nation's most well-known investigative reporter with an intelligence beat.

Intelligence studies has come of age.

Certainly the chapters in these volumes display a breadth of inquiry that suggests an admirable vibrancy in this relatively new field of study. Presented here are empirical inquiries, historical treatments, theoretical frameworks, memoirs, case studies, interviews, legal analyses, comparative essays, and ethical assessments. The authors come from the ranks of academe (twenty-five); the intelligence agencies (thirteen); think tanks (seven); Congress, the State Department, and the National Security Council (three); and the legal world (three).[1] Over a quarter of the contributors are from other nations, including Canada, England, Germany, Israel, Scotland, Switzerland, and Wales. The American writers come from every region of the United States. As a collective, the authors represent a wide range of scholarly disciplines, including computer science, history, international affairs, law, sociology, political science, public administration, public policy studies, and strategic studies. Many of the contributors are from the ranks of the top intelligence scholars in the world; a few young ones stand at the gateway to their academic careers.

Notable, too, is the number of women who have entered this field of study. Thirty years ago, it would have been rare to find one or two women writing on this subject. Seven have contributed chapters to these pages, and another two wrote documents that appear in the appendixes. This is still fewer than one would like, especially in light of the major contribution women have made as intelligence officers. One thinks of the heroic efforts of British women in code breaking and in the Special Operations Executive during World War II, and the American women who contributed so much to the analytic efforts of the Office of Strategic Studies (OSS) during that same war. At least, though, the number attracted to the scholar study of intelligence appears to be rapidly expanding.

The end result of this mix is a landscape illuminated by a variety of methods and appreciations—a rich research trove that examines all the key aspects of intelligence. In addition, each of the volumes contains backup materials in the appendixes. These documents provide the reader with access to significant primary and secondary sources referred to in the chapters.

The volumes are organized according to the major topics of studies in the field. The first volume, titled *Understanding the Hidden Side of Government*, introduces the reader to methods commonly used in the study of intelligence. It imparts, as well, a sense of the "state of the discipline," beginning with a bibliographic essay (by the editor) and continuing with an examination of specific approaches scholars have adopted in their inquiries into this especially difficult discipline, where doors are often shut against outsiders.

In the bibliographic essay that opens the volume, I argue that the literature on intelligence has mushroomed over the past thirty years. Some of this literature is unreliable, but much of it is of high quality. Amy B. Zegart follows my chapter with an important caveat: the literature may be more voluminous these days, but intelligence studies as an academic field has yet to be accepted as a vital part of national security scholarship. The mainstream journals of history, international

affairs, and political science have still regarded the study of intelligence as a marginal pursuit. In this regard, Zegart points out, there is a major disconnect between academic scholarship and those who make decisions in Washington, London, and other capitals around the world.

Following this introduction, Len Scott and Timothy Gibbs look at methods that have been used to study intelligence in the United Kingdom; Stuart Farson and Reg Whitaker in Canada; and Michael Warner in the United States. The volume then turns to a more specific inquiry into the central question of how intelligence is interpreted by professionals—the issue of analysis—explored by John Hollister Hedley. An overview of the sometimes turbulent relationship between intelligence officers and the policy makers they serve is explored by James J. Wirtz; and British scholar Peter Gill recalls the failures associated with the 9/11 attacks and the poor judgments about Iraqi WMDs, in hopes of extracting lessons from these intelligence disasters. In the next chapter, the youngest scholar represented in this collection, Harold M. Greenberg, takes us back in time with a remembrance of the legendary CIA officer and Yale history professor Sherman Kent, often known as the dean of CIA analysts. Kristin Lord rounds out the first volume with a look forward into future prospects for a more transparent world—the ultimate goal of intelligence.

As with each of the books, Volume 1 has a set of appendixes designed to supplement the original chapters with supportive materials from government documents and other sources. Appendix A contains the relevant intelligence excerpts from the National Security Act of 1947—the founding charter for the modern American intelligence establishment. Appendix B provides a history of U.S. intelligence since 1947, prepared for the Aspin-Brown Commission in 1995–96 by staff member Phyllis Provost McNeil. These two documents present a contextual backdrop for the Volume 1 chapters. Appendix C provides "wiring diagrams" of the intelligence community, that is, organizational blueprints for the sixteen agencies and related entities. One chart displays the community as it is today, and another displays how it looked in 1985. As the contrast between the two illustrates, the events of September 11, 2001, have led to a larger and more complex intelligence apparatus in the United States. Appendix D shows a photograph of the CIA Headquarters Building, as an example of what one of the secret agencies actually looks like from an aerial perspective. The white dome in the foreground is an assembly hall seating around 600 people and to its left is the main entrance to the original CIA headquarters, built during the Eisenhower years. Behind this older wing is the new green-glass structure erected during the Reagan administration, often known as the Casey addition because William J. Casey was the Director of Central Intelligence (DCI) at the time of its construction during the 1980s.

Appendix E lists the top leadership in the America's intelligence community: the DCIs from 1947–2005 and today's DNI. Included here as well are the leaders in Congress who have been responsible for intelligence accountability in the past, along with the current members of the two congressional Intelligence

Committees: the Senate Select Committee on Intelligence (SSCI, or "sissy" in the unflattering and sometimes true homophone of Capitol Hill vernacular) and the House Permanent Select Committee on Intelligence (HPSCI or "hipsee"). Appendix F presents a 1955 statement from historian and CIA analyst Sherman Kent about the need for a more robust intelligence literature. He would probably be amazed by how much is being written on this subject now. Appendix G offers an overview on the purpose and challenges of intelligence, drawn from the introductory chapters of the Aspin-Brown Commission Report. Finally, Appendix H provides an opening glimpse into the subject of counterintelligence, a world of counterspies and betrayal taken up more fully in Volume 4.

With the second volume, titled *The Intelligence Cycle: The Flow of Secret Information From Overseas to the Highest Councils of Government*, the focus shifts from a broad overview of intelligence to a more detailed examination of its core mission: the collection, analysis, and dissemination of information from around the world. The National Security Act of 1947, which created America's modern intelligence establishment, made it clear that the collection, analysis, and dissemination of information would be the primary duty of the intelligence agencies. As Allen Dulles—the most famous DCI (America's top intelligence official, until this title changed to director of National Intelligence or DNI in 2005)—put it, the intelligence agencies were expected "to weigh facts, and to draw conclusions from those facts, without having either the facts or the conclusions warped by the inevitable and even proper prejudices of the men whose duty it is to determine policy."[2] The collection and interpretation of information, through espionage and from the public record, would be the primary responsibility of America's secret agencies.

At the heart of this mission lies the so-called intelligence cycle. Professional intelligence officers define the cycle as "the process by which information is acquired, converted into intelligence, and made available to policymakers."[3] The cycle has five phases: planning and direction, collection, processing, production and analysis, and dissemination (see Appendix A in Volume 2 for a depiction). As former CIA officer Arthur S. Hulnick notes, however, in the opening chapter, the idea of a "cycle" fails to capture the complexity of how intelligence is collected, assessed, and distributed by intelligence officers.

The next five chapters in Volume 2 take us into the world of the "ints," that is, the specialized "intelligences" (methods) used by intelligence officers to collect information. Patrick Radden Keefe and Matthew M. Aid probe the method of signals intelligence or SIGINT, a generic term used to describe the interception and analysis of communications intelligence and other electronic emissions, from wiretapping telephones to studying the particles emitted by missiles in test flights. Both authors are sensitive to the possible abuse of these techniques, which can be and have been used to spy on Americans without a proper judicial warrant. Jeffrey T. Richelson explores the IMINT domain, that is, imagery intelligence or, in simple terms, photographs taken by surveillance satellites and reconnaissance airplanes (piloted and unpiloted). Telephone conversations can be revealing, but

in the old saying, a picture can be worth a thousand words. (Appendix B provides photographic examples of these spy platforms, and Appendix C offers illustrations of the IMINT data they can collect.)

Important, too, is information that can be acquired by human agents ("assets") guided by case officers inside the CIA or the Defense Department, the topic of human intelligence or HUMINT, examined by Frederick P. Hitz. Not all the information needed by policy makers is acquired through SIGINT, IMINT, or HUMINT; indeed, the overwhelming majority—upward of 95 percent—is already in the public domain. This open-source intelligence (OSINT) must be sorted through, organized, and integrated with the secretly gained information. Robert David Steele's chapter looks at OSINT and its ties to the other ints.

In the next chapter, Daniel S. Gressang IV dissects some of the technological challenges faced by intelligence agencies in sorting through the avalanche of data that pours into their headquarters from various intelligence collectors around the world. Here is the Herculean task of sorting out the wheat from the chaff (or the signal from the noise, in another widely used metaphor) in the search for information that may warn the nation of impending peril. Here is the vital task of providing "indicators and warnings" (I&W) to a nation's leaders.

One of the most difficult relationships in the complex process of collection, analysis, and dissemination of information comes at the intersection between intelligence professionals and policy makers—groups of individuals that often have very different training, aspirations, and cultures. Jack Davis sheds light on this often turbulent relationship in the United States, and Michael Herman tackles the same topic in the United Kingdom. Minh A. Luong offers a case study on economic intelligence that underscores some of the difficulties encountered as information travels from the collectors and analysts (the "producers" of intelligence) to the policy makers (the "consumers"). Finally, Max M. Holland takes a look at how intelligence agencies examine their own mistakes ("postmortems") and attempt to make corrections—and how political consideration enter into the process.

By way of supporting documentation, in addition to the appendixes already mentioned, Appendix D outlines the general types of reports prepared by the producers of intelligence, along with a listing of specific examples. Appendixes E and F provide samples of key intelligence products: National Intelligence Estimates (NIEs)—the most important long-range and in-depth forecasting carried out by the U.S. secret agencies ("research intelligence," in contrast to shorter intelligence reports that tend to focus on near-term events, or "current intelligence"); Special National Intelligence Estimates (SNIEs), which concentrate on a narrow, high-priority information requirement (say, the capabilities of the Chinese military); and the *President's Daily Brief* (PDB), the most exclusive current intelligence report prepared by the intelligence agencies for the consumption of the president and a few other high-ranking officials.

In light of the fact that every study of the 9/11 and Iraqi WMD intelligence failures find fault, in part, with America's capacity for human intelligence—

especially in the Middle East and Southwest Asia—Appendix G presents one of the most searing critiques of this int. The critique, by the House Permanent Select Committee on Intelligence, has become all the more significant because the panel's chairman, Representative Porter Goss (R-FL), soon after the completion of the report rose to the position of the DCI. Last, Appendix H provides an excerpt from a key report on the Iraqi WMD mistakes, prepared by the "Roberts Committee": the Senate Select Committee on Intelligence, led by Pat Roberts (R-KS).

The third volume, titled *Covert Action: Behind the Veils of Secret Foreign Policy*, enters an especially controversial compartment of intelligence: the means by which the United States attempts to not just gather and analyze information about the world—hard enough—but to manipulate global events through secret activities in the advancement of America's best interests. An ambiguous passage of the National Security Act of 1947 charged the National Security Council (NSC), the boss over the sixteen U.S. secret agencies, to "perform such other functions and duties related to intelligence [over and beyond collection-and-analysis] affecting the national security as the National Security Council may from time to time direct."[4] The phrase "other functions and duties" left the door open for launching the CIA (and more recently the Pentagon) on a wide range of covert actions around the world.

Covert action (CA), sometimes referred to as the "quiet option," is based on the supposition that this secret approach to foreign affairs is likely to be less noisy and obtrusive than sending in the Marines. Sometimes professional practitioners also refer to covert action as the "third option," between diplomacy and open warfare. As former Secretary of State and National Security Adviser Henry Kissinger once put it: "We need an intelligence community that, in certain complicated situations, can defend the American national interest in the gray areas where military operations are not suitable and diplomacy cannot operation."[5] Still others prefer the euphemism "special activities" to describe covert action. Whatever the variation in terminology, the goal of covert action remains constant: to influence events overseas secretly and in support of American foreign policy.

Covert action operations are often grouped according to four broad categories: propaganda, political, economic, and paramilitary (PM) activities. An example of a propaganda operation was the CIA's use of Radio Free Europe during the Cold War to transmit anti-communist themes into nations behind the Iron Curtain. A political CA during the Cold War was the CIA's clandestine funneling of funds to the anti-communist Christian Democratic Party in Italy. An economic example: the CIA attempted to destroy electric power stations in Nicaragua during the 1980s, as a means of undermining the Marxist-oriented S*andinista* regime. PM operations can including everything from assassination plots against foreign heads of state to arming and guiding pro-American insurgent armies in one country or another. Little wonder this has been a controversial subject.

Gregory F. Treverton introduces the reader to covert action in the first chapter of Volume 3. He is followed by Kevin A. O'Brien and Ephraim Kahana, who discuss the use of covert action by other nations. The next four chapters illuminate certain aspects of CA, with James M. Scott and Jerel A. Rosati providing an overview of CA tradecraft (that is, the tools used to implement such operations); Michael A. Turner evaluating the merits of CIA covert propaganda operations; William J. Daugherty looking at political and economic examples of covert action; Jennifer D. Kibbe exploring the entry of the Defense Department into this domain; and former diplomat John D. Stempel contrasting the uses of covert action to diplomatic initiatives. Winding up the volume is Judge James E. Baker's legal analysis of covert action.

Supporting documents include excerpts from the Church Committee Report on the evolution of covert action as carried out by the CIA (Appendix A). The supervision of covert action went from an informal to a highly formal process, as a result of a law known as the Hughes-Ryan Act, passed on December 31, 1974. The language of this statute is presented in Appendix B, and the covert action procedures that resulted from the law are outlined in Appendix C. At the center of the covert action decision process since the Hughes-Ryan Act is the *finding*, a term of art that stems from the passage in the law that requires the president to "find" that a particular covert action proposal is important and has the president's approval. Appendix D contains two findings from the Iran-*contra* era in the mid-1980s. Covert actions must have an organizational apparatus to carry them out, and Appendix E displays what that apparatus looked like during the Cold War (and in basic form remains the organizational chart today, with a few name changes in the boxes).

One of the most controversial forms of covert action has been the assassination of foreign leaders. Appendix F presents a case study from the Church Committee on the CIA assassination plot hatched against the leader of the Republic of Congo, Patrice Lumumba, in 1960. The Committee's exposé of this and other plots led President Gerald R. Ford to sign an executive order prohibiting assassination as an instrument of American foreign policy (see Appendix G). The executive order has been waived in times of authorized warfare against other nations, however, leading to failed attempts to assassinate Saddam Hussein in the first and second Persian Gulf Wars (he was eventually captured alive in 2004, hidden away in a hole near his hometown in Iraq) and Al Qaeda leader Osama bin Laden during the Clinton administration. Considerable ambiguity exists regarding the current status of the executive order and under what conditions it might be waived by administrations. Finally, Appendix H—drawing on a presidential commission study and congressional hearings—examines covert action at its lowest state: the Iran-*contra* affair of the 1980s, when this approach to foreign policy subverted the U.S. Constitution and several laws (including the Hughes-Ryan Act).

A third intelligence mission, after collection-and-analysis and covert action, is counterintelligence (CI) and its associated activity, counterterrorism (CT).

Here is the concentration in Volume 4, titled *Counterintelligence and Counterterrorism: Defending the Nation Against Hostile Forces*. Like covert action, CI went without specific mention in the National Security Act of 1947. By the early 1950s, however, it had similarly achieved a status of considerable importance as an intelligence mission. CI specialists soon waged nothing less than a secret war against antagonistic intelligence services (especially the Soviet KGB); and, after the Cold War, CT specialists would focus on efforts to block terrorists who targeted the United States and its allies. Explaining why the mission of counterintelligence/counterterrorism evolved, a CI expert has pointed out that "in the absence of an effective U.S. counterintelligence program, [adversaries of democracy] function in what is largely a benign environment."[6]

The practice of counterintelligence consists of two matching halves: security and counterespionage. Security is the passive or defensive side of CI, involving such devices as background investigations, fences, sentries, alarms, badges, watchdogs, and polygraphs (lie detection machines). Counterespionage (CE) is the offensive or aggressive side of CI. The most effective CE operation is the infiltration of an American agent or "mole" into the enemy camp, whether a hostile intelligence service or a terrorist cell—a ploy called a penetration. Thus, the practice of security is, according to one of America's top counterintelligence experts, "All that concerns perimeter defense, badges, knowing everything you have to know about your own people," whereas the CE side "involves knowing all about intelligence services—hostile intelligence services: their people, their installations, their methods, and their operations."[7]

Stan A. Taylor and Nigel West clarify these issues in the first two chapters of this volume, then in the next two chapters Katherine A. S. Sibley and Athan Theoharis examine the challenges of keeping the United States spy-free. Rhodri Jeffreys-Jones looks at the efforts in Europe to create a counterintelligence capability similar to that practiced by America's Federal Bureau of Investigation (FBI). Glenn Hastedt takes the reader into the counterterrorism thicket in Washington, DC, explaining how politics influences CI and CT operations. Richard L. Russell and Jennifer Sims discuss the ups and downs of trying to establish an effective counterterrorism response in the United States, complicated by the fragmentation of authority and widely differing cultures among the sixteen U.S. intelligence agencies. Finally, Katharina von Knop looks at the rising role of women in terrorist organizations.

The back-of-the-book documents in Volume 4 begin with a look at the Church Committee findings regarding counterintelligence in 1975 (Appendix A), followed by the notorious Huston Plan—a master counterintelligence spy plan drafted by White House aide Tom Charles Huston in 1970, in response to a nation at unrest over the war in Vietnam (Appendix B). The Huston Plan is a classic illustration of overreaction in a time of domestic strife. In Appendix C, the Senate Select Committee on Intelligence summarizes its findings about the Aldrich H. Ames counterintelligence disaster. Next the appendixes include a series of U.S. commission conclusions about how to improve intelligence in the struggle

against global terrorism, whether locating and penetrating their cells in advance of a terrorist attack or thwarting the ability of terrorists to acquire WMDs. The panel reports include: the Hart-Rudman Commission of 2001 (Appendix D); the 9/11 or Kean Commission of 2004 (Appendix E); and the Silberman-Robb Commission of 2005 (Appendix F). For purposes of comparison, the final appendix (G) examines the conclusions reached by a British commission that also probed the Iraqi WMD failure: the Butler Report of 2004.

The fifth volume in the series, titled *Intelligence and Accountability: Safeguards Against the Abuse of Secret Power*, stems from a concern that secret power might be misused by those in high office. This danger was underscored in 1975 when Congress found the U.S. intelligence agencies guilty of spying against law-abiding American citizens, and again in 1987 during the Iran-*contra* affair when some elements of the intelligence community violated the public trust by ignoring intelligence laws. The United States has been one of the few nations in the world to conduct an ongoing experiment in bringing democratic accountability to secret government activities. Democracy and spying don't mix well. Secrecy runs counter to democratic openness, while at the same time openness possesses a threat to the success of espionage operations. Democracies need intelligence agencies to acquire information that may protect them, but thoughtful citizens worry about having secret agencies in an open society.

Until 1975, the nation's remedy for the tension between intelligence gathering and democracy was to trust the intelligence agencies and hope for the best. Elected officials treated the secret services as exceptional organizations, immune from the checks and balances envisioned by the framers of the Constitution. Lawmakers were satisfied with this arrangement, because if an operation went awry they could duck responsibility. When James R. Schlesinger, DCI in 1973, attempted to inform John Stennis (D-MS), a key member of the Senate Armed Services Committee, about an approaching operation, the Senator stopped him short: "No, no, my boy, don't tell me. Just go ahead and do it, but I don't want to know."[8]

This attitude on Capitol Hill—overlook rather than oversight—underwent a dramatic turnabout in December 1974, however, when the *New York Times* reported on allegations of CIA spying at home and questionable covert actions in Chile. Congress might have waved aside the revelations about Chile as just another Cold War necessity in the struggle against regimes leaning toward Moscow, but spying on American citizens—voters—was another matter altogether. In January 1975, President Ford created the Commission on CIA Activities Within the United States (the Rockefeller Commission, led by his vice president, Nelson Rockefeller). Later that month the Senate established a select committee to investigate intelligence activities. The committee was headed by Frank Church, D-ID, and became known as the Church Committee (the editor served as Church's assistant). A counterpart House committee, led by Representative Otis Pike (D-NY), began investigations the following month.

These various panels, especially the Church Committee, found many more improprieties than they had expected. Not only had the CIA engaged in domestic

spying in violation of its charter, so had the FBI and several military intelligence units. Furthermore, the FBI had carried out secret operations, known collectively as COINTELPRO, against thousands of civil rights activists, members of the Ku Klux Klan, and Vietnam War dissenters. The objective was to make their lives miserable by disrupting their marriages and employment. The Bureau even attempted to blackmail Dr. Martin Luther King Jr. into committing suicide. Church Committee investigators also discovered CIA assassination plots against foreign leaders and efforts to topple President Salvador Allende of Chile, even though he had been democratically elected.

These revelations convinced lawmakers that the time had come to bring accountability into the dark recesses of government. Congress established intelligence oversight committees in both chambers—the Senate in 1976 and the House a year later—and, by 1980, required by law timely reports on all secret intelligence operations. The new Committees pored over intelligence budgets, held regular hearings (mostly in closed session to protect spy sources and methods) and seriously examined the performance of America's intelligence agencies. No other nation has ever so thoroughly applied democratic principles to its secret services, although a number are now beginning to follow the leadership of the United States toward greater intelligence supervision.[9]

Since 1975, this effort has evolved in fits and starts. Sometimes lawmakers have insisted on close accountability, as when they enacted the Intelligence Oversight Act of 1980 with its stringent reporting requirements for covert operations, or when a series of laws in the 1980s sought to end covert actions in Nicaragua. At other times, members of Congress have loosened the reins—for example, repealing in 1985 a prohibition against covert action in Angola. On still other occasions, Congress has concentrated on helping the intelligence agencies improve their security and performance, as with a law in 1982 that prohibited exposing the names of undercover officers. The Iran-*contra* scandal of 1987 was a major setback to this new oversight, as the Reagan administration bypassed most of these rules and statutes in its conduct of a covert war in Nicaragua against the will of Congress. The scandal was an alert to lawmakers. The Intelligence Oversight Act of 1991 further tightened intelligence supervision by clarifying reporting requirements. Lawmakers also set up an Office of Inspector General in the CIA, confirmed by and accountable to Congress.

The pulling and tugging has continued, most recently over whether President George W. Bush violated the Foreign Intelligence Surveillance Act (FISA) of 1978 by conducting warrantless wiretaps as part of the war against terrorism in the aftermath of the 9/11 attacks. The FISA required warrants, but the White House claimed (when the secret operation leaked to the media) the law had become to cumbersome and, besides, the president had inherit authority to conduct the war against terrorism as he saw fit. This debate aside for the moment (several authors address the issue in these volumes), one thing is certain: the intelligence agencies in the United States are now very much a part of the nation's system of checks and balances. Americans want and deserve both civil liberties and a secure defense

against threats; so the search continues for an appropriate balance between liberty and security, democracy and effectiveness—precisely the topic of Volume 5.

The set of chapters on intelligence accountability are introduced with a chapter by David M. Barrett, the foremost authority on the history of accountability in the early years of modern U.S. intelligence (1947 to 1963). The chief counsel of the Church Committee, Frederick A. O. Schwarz Jr., then reflects back on the effects of that watershed inquiry. Next, the editor offers a previously unpublished interview with DCI William E. Colby, who stood at the helm of the intelligence community as it weathered the storm of the investigations into domestic spying during 1975. Mark Phythian presents a chapter on the British experience with intelligence accountability; and, comparing British and American oversight, Lawrence J. Lamanna contrasts the responses on both sides of the Atlantic to the faulty Iraqi WMD assessments in 2002.

The next chapter, written by Cynthia M. Nolan, looks at contemporary issues of intelligence oversight in the United States. Hans Born and Ian Leigh follow with a comparative dimension by contrasting intelligence accountability practices in a variety other nations. Finally, A. Denis Clift and Harry Howe Ransom, who have witnessed the unfolding of intelligence accountability over the past four decades, offer their appraisals of where the experiment stands today.

The first supporting document in this volume is a succinct legislative history of intelligence accountability from 1947 to 1993, prepared by the Senate Select Committee on Intelligence (Appendix A). Then come a series of important oversight laws, beginning with FISA in 1978. With this law, members of Congress sought to rein in the open-ended authority of the executive branch to wiretap and otherwise spy on individuals considered risks to the national security—a privilege abused by a number of administrations from the 1930s forward. Henceforth, FISA required a warrant from a special court (the FISA Court, whose members are appointed by the Chief Justice of the Supreme Court) before such intrusive measures could be carried out. This law, a hot topic in 2005–6 when critics charged the second Bush administration with violation of the warrant requirement, can be found in Appendix B.

The Intelligence Oversight Act of 1980 is presented in Appendix C. This is a brief but nonetheless far-reaching law, enacted by Congress as an attempt to become an equal partner with the executive branch when it came to intelligence. The 1991 Intelligence Oversight Act (Appendix D) emerged after the Iran-*contra* scandal and provided a tightening and clarification of the language in its 1980 precursor, especially with respect to the approval and reporting rules for covert action. The political tug-of-war over the drafting of this currently prevailing oversight statute was intense, leading to the first and only presidential veto of an intelligence act. President George H. W. Bush found the proposal's insistence on prior reporting of covert action objectionable in times of emergency. Lawmakers entered into a compromise with the chief executive, settling on a two-day reporting delay in emergencies. The bill passed Congress again, this time without a presidential veto.

In 1995, the House Permanent Select Committee on Intelligence launched an inquiry into a wide assortment of intelligence issues, stimulated initially by counterintelligence concerns (Aldrich Ames's treasonous activities at the CIA had recently been discovered) but turning into an opportunity for a broad review of new challenges that faced the secret agencies now that the Cold War had ended. In Appendix E, an excerpt from the Committee's final report examines the state of intelligence accountability in the mid-1990s. The next document, in Appendix F, carries the examination into the twenty-first century, with the appraisal of the 9/11 Commission on the same subject. The commissioners were unimpressed, referring to intelligence accountability as "dysfunctional."

At the center of any efforts to maintain accountability for the secret agencies lies the question of funding—the mighty power of the pursue, held in the hands of lawmakers. Appendix G draws on the findings of the Aspin-Brown Commission to provide official documentation about how the United States spends money for spying. Finally, in Appendix H, DCI Robert M. Gates (1991–93) offers observations about oversight from the perspective of the intelligence community management team, located at that time on the Seventh Floor of the CIA.

Here, then, is what the reader will find in these five volumes. The editor and the contributors hope the chapters and documents will help educate the public about the importance of intelligence agencies, as well as stimulate scholars around the world to further the blossoming of this vital field of study. I am pleased to acknowledge my gratitude to Praeger's Heather Staines, senior project editor, and Anne Rehill, development editor, each a pleasure to work with and most helpful in their guidance; Julie Maynard at the University of Georgia for her administrative assistance; Lawrence J. Lamanna, my graduate research assistant, for his good counsel and logistical help; Leena S. Johnson for her indispensable encouragement and support; and the contributors to these volumes for their outstanding scholarship and their much appreciated cooperation in keeping the publishing train running on time.

These volumes are enthusiastically dedicated to Harry Howe Ransom, who has done so much in the United States to lead the way toward a serious discipline of intelligence studies.

Loch K. Johnson

NOTES

1. Some of the authors have had multiple careers, so in categorizing them I have counted the place where they have spent most of their professional lives.

2. Quoted by Senator Frank Church (D-ID), in *Congressional Record* (January 27, 1976), p. 1165.

3. *Fact Book on Intelligence* (Washington DC: CIA Office of Public Affairs, April 1983), p. 17.

4. National Security Act of 1947, signed on July 26, 1947 (P.L. 97-222; 50 U.S.C. 403, Sec. 102).

5. Comment, "Evening News," NBC (January 13, 1978).

6. Editor's interview with a FBI counterintelligence specialist, Washington, DC (May 16, 1975).

7. Editor's interview with Raymond Rocca, CIA/CI specialist, Washington, DC (November 23, 1975).

8. Editor's interview with James R. Schlesinger, Washington, DC (June 16, 1994).

9. See Hans Born, Loch K. Johnson, and Ian Leigh, *Who's Watching the Spies? Establishing Intelligence Service Accountability* (Washington, DC: Potomac Books, 2005).

1

CONGRESSIONAL OVERSIGHT OF THE CIA IN THE EARLY COLD WAR, 1947–63

DAVID M. BARRETT

INTRODUCTION

A DEMOCRATIC NATION-STATE IN A DANGEROUS WORLD faces two obvious dilemmas that might be labeled "openness versus secrecy" and "fair play versus dirty tricks." *Openness* is at the heart of democratic theory and practice. If a nation's government is not substantially open about what it is doing and how it is doing it, then that nation's citizens can hardly pass effective judgment about the government in periodic elections. However, in a world full of perils, any government must employ much secrecy about its military and intelligence capabilities and plans.

Meanwhile, many citizens and leaders of democratic nation-states—certainly the United States—consider themselves to believe in fair play. President George Washington's famous farewell address set a standard along these lines by calling for the U.S. government to follow "exalted virtue" in its dealings with other nations. This, he predicted, would ultimately lead other nations to become habituated toward doing the right thing in their foreign affairs.

This is not to say that U.S. foreign policy was consistently virtuous across the ensuing decades. A century and a half later, a secretive commission advising President Dwight Eisenhower explicitly parted company with Washington. The world had become uniquely dangerous, due to the expansionist, communist, and nuclear-armed Soviet Union, "an implacable enemy whose avowed objective is world domination by whatever means and whatever cost. . . . If the United States is to survive, longstanding concepts of 'fair play' must be reconsidered." The United States would have "to learn to subvert, sabotage, and destroy our enemies

by more clever, more sophisticated, and more effective methods than those used against us." Dirty tricks were necessary.[1]

Solutions to these two dilemmas were and are imperfect, to say the least. Still, they are at least mitigated for the United States by having some constitutionally elected leaders know of and give direction to covert action, espionage, and other morally unsavory policies. Most obviously, the President—having the executive power and commander-in-chief roles—should carry out such duties. The U.S. Constitution, though, gives the Congress the law-making power (shared with a veto-endowed President), which includes the right the pass spending laws. In light of this, during Washington's presidency, Congress first asserted a constitutionally implied right to monitor and investigate executive branch agencies.

THE LITERATURE ON CONGRESS AND THE CIA IN EARLY COLD WAR YEARS

Writings on Congress and the Central Intelligence Agency (CIA) in the Truman-Eisenhower-Kennedy era have been very few in number. Harry Howe Ransom provided rare early and thoughtful scholarly treatments of legislative oversight in books and articles on CIA, finding in 1958 that the agency operated "with only nominal legislative surveillance."[2] Despite his best efforts to learn details of CIA-Congress relations, Ransom was handicapped by the secrecy surrounding the agency. A later and more extensive (retrospective) treatment of the topic came from the Church Committee of the mid-1970s, named for its chairman, Senator Frank Church (D-ID). That committee came into being as a result of various published allegations in the *New York Times* and certain books concerning certain questionable actions of the CIA in previous decades. Though the committee's main focus was not on legislative oversight of CIA, it did give substantially more attention to the topic than had occurred before. It found that "from the beginning," the House and Senate subcommittees charged with monitoring the CIA "were relatively inactive."[3] Newspapers and magazines in the United States sporadically paid attention to congressional oversight of CIA in the early Cold War years. An early example was the Richmond *News-Leader,* which charged Congress in the early 1950s with ignoring the CIA's "free-wheeling" status.[4]

Working from much fuller evidence that has become available in the past decade, it is fair to say that the two adjectives that best describe congressional oversight of the CIA during the Truman, Eisenhower, and Kennedy eras are *limited* and *informal*. This is especially so when that oversight is compared to the oversight that Congress instituted and has carried out from the mid-1970s through the early 21st century. In the modern era, there are many hundreds of interactions between Capitol Hill and the CIA per year; the House and Senate Intelligence Committees are large and have substantial staffs. By contrast, from 1947—when the CIA was created by President Truman and Congress—through the early 1960s, there were anywhere from eight to thirty hearings held each year.

There were scores of other interactions between individual legislators and CIA personnel annually. But the hearings and the smaller, more informal sessions were almost all carried out under conditions of extreme secrecy. The legislators who conducted them were mostly on four tiny House and Senate Appropriations and Armed Services subcommittees that were mandated to monitor the CIA. Those legislators were assisted in these tasks by a small number of staff assistants, none of whose jobs were exclusively devoted to intelligence affairs.

Still, most of the literature on Congress and the CIA has been erroneous in asserting that there was virtually no intelligence oversight in the early Cold War era, especially by the late Eisenhower era. Claims are common that Director of Central Intelligence (DCI) Allen Dulles (1953–61) only had jocular but shallow meetings with legislators. Dulles's own experience of legislative oversight is instructive: In 1958, he spent parts of at least twenty-five days on Capitol Hill. There, he met with ten or more different committees or subcommittees. During his long tenure and afterward, he periodically clamed that legislative oversight of the CIA had been reasonably substantive, though few have taken his claim seriously.[5]

The political atmosphere was challenging for Dulles in a year like 1958. For example, many Congress members had publicly expressed doubts that CIA had alerted President Eisenhower and others that (1) the Soviet Union was likely to launch an earth satellite in the autumn of 1957, that (2) Venezuelans were likely to riot and almost kill Vice President Richard Nixon on a "good will" visit to that country, or that (3) the pro-American government of Iraq would be overthrown by a coup, thus provoking American intervention in nearby Lebanon. Dulles was relatively honest with legislators in that year's secret hearings, responding that CIA had alerted President Eisenhower and at least one congressional subcommittee that the USSR might launch an earth satellite in 1957, that CIA had relied too much on Venezuelan security services for its intelligence on the dangers Nixon might face, and that the Agency had simply failed to anticipate the Iraqi coup. In the next few years, following the U-2 and Bay of Pigs incidents, CIA's challenges on Capitol Hill would be greater.[6]

One element missing from most of the literature on Congress and the CIA is treatment of a particular kind of accountability that existed: DCIs Roscoe Hillenkoetter (1947–50), Walter B. Smith (1950–53), Dulles, and John McCone (1962–65) literally feared what congressional barons heading the CIA subcommittees might do to the Agency if its leader were discovered to have lied or refused directives received on Capitol Hill. (The intelligence directors met those powerful legislators privately more often than they did in subcommittee sessions. Such meetings were poorly documented, unfortunately.) When Vice President Lyndon Johnson warned McCone in 1962 that Armed Services Committee chair Richard Russell (D-GA)—who was the most knowledgeable senator about CIA affairs—could "destroy" the Agency and McCone if he were not responsive on a current controversy, the DCI was being told something that he already knew. By virtually all accounts of those who worked for the four directors, keeping the

members (especially chairs and ranking minority members) of the CIA subcommittees satisfied was of prime importance.[7]

This is not to say that the Agency faced anything like systematic scrutiny by Congress over its first decade and a half. As CIA legislative liaison John Warner occasionally pointed out to colleagues, the leaders of the CIA subcommittee were often too busy to pay as much attention to the Agency as they should have.

ESSENTIAL FEATURES OF CIA OVERSIGHT BY CONGRESS, 1947–63

Within a year of the CIA's creation in 1947, the House and Senate Armed Services and Appropriations Subcommittees began emerging and holding informal hearings with Agency leaders present. The frequency of those sessions in the late 1940s was low, and they have never been well documented. It was inevitable that the Appropriations Subcommittees (not formally named, but occasionally referred to by members simply as the "CIA Subcommittees") would come into being, because the CIA needed funds, but no one at the Agency, on Capitol Hill, or at the White House wanted the full Appropriations Committees to have access to information on the new Agency. CIA was already doing analysis and coordination of the writing of estimates; also, some of its personnel were doing espionage and covert action. Thus, during the Agency's first few years, no more than five Appropriations members at the House and fewer than three at the Senate knew any details about CIA's budgets, which were moving upward toward the $100 million mark.[8]

The Armed Services Committees successfully asserted their claims as the relevant law-making bodies to deal with CIA-related issues. But their chairs had no more interest than the Appropriations leaders in having all Committee members interact with CIA. The commonly expressed view—both in public and in private—was that CIA's work was too important for it to be endangered by leaks to the press, which would, in turn, inform the Soviet Union of such information. The resulting subcommittees were also small and met as infrequently as one to four times per year in the late 1940s.

Though the frequency of hearings and other meetings of the CIA subcommittees grew substantially in the 1950s and 1960s, certain features remained constant across the Truman, Eisenhower, and Kennedy eras. One was the dominance of their chairmen and ranking minority members. In the Senate, the chairs of the committees also headed the CIA subcommittees. In the House, this was also the case until the late 1950s, when the Armed Services and Appropriations Committee chairs—Democrats Carl Vinson (GA) and Clarence Cannon (MO)—turned over their CIA subcommittee chairmanships to Paul Kilday and George Mahon, both Texas Democrats. Nonetheless, Vinson and Cannon usually attended subcommittee meetings.

There seems to have been greater knowledge on the part of chairs and ranking minority members than there was among the other subcommittee members. In the Appropriations Subcommittees, for example, a few years passed before leaders informed other members of the existence of the U-2 program, which sent spy flights across the Soviet Union. This conforms to what Stephen Horn later wrote: the chairs and ranking minority members of Senate Appropriations were "lord and masters" of the Committee.[9]

Another feature of the subcommittees' dynamics was the lack of partisanship. Relations between the majority and minority party leaders and members were trusting and respectful most of the time. This made it "a joy to work there," said Bill Darden, a leading staffer at the Senate Armed Services Committee. Also, on those occasions in the 1940s and 1950s when party control of Congress changed, most staffers who interacted with CIA frequently (like Darden) stayed on in their jobs. There were not many such staff members, though. In any given year, fewer than ten of them—from the four subcommittees and the occasional other committee that looked into CIA matters—were designated by their bosses to do such work. With few exceptions (especially Senator Styles Bridges [R-NH], who was an ally of powerful columnist Drew Pearson), neither staffers nor members of the CIA subcommittees leaked to the press.

DID SUBCOMMITTEE MEMBERS KNOW THE CIA'S INTIMATE SECRETS?

Covert Action

Contrary to what is commonly found in the literature, it is clear that subcommittee leaders and/or members knew a fair amount about covert action. This should not be surprising: Congress members, whether they were on CIA subcommittees or not, mostly favored aggressive action. Records that have been uncovered in recent years show that many legislators went to executive branch leaders and suggested covert action in various parts of the world. "Why don't we instigate a large program of stirring up guerrilla activity on the Chinese mainland?" asked one out-of-the-loop legislator in 1950. Indeed, such Congress members who were not knowledgeable about the CIA managed to pass an amendment in 1951 that handed $100 million to the Truman administration to try to "roll back" Soviet influence in Eastern Europe. The money was not used because it was not needed by CIA, which was then funded by the House and Senate Appropriations CIA subcommittees at a level of almost half a billion dollars, much of it for covert action.[10]

Two of the best remembered covert actions of the early Cold War era were the removal of the left-leaning government of Guatemala in 1954 (during the Eisenhower presidency) and the wildly unsuccessful attempt to overturn Fidel Castro's government of Cuba in 1961's Bay of Pigs incident (during the Kennedy

presidency). Did the CIA subcommittee members and/or other legislators have advance knowledge of those planned covert actions? The evidence regarding Guatemala is extremely fragmentary, but it is likely that at least the heads of the subcommittees and some other legislators knew of those plans in advance. Furthermore, leaders at the CIA and elsewhere in the executive branch felt heat from Congress, who feared a Latin American outpost of the Soviet Union enough to insist that the executive branch "do something" about Guatemala.

As for the Bay of Pigs invasion, two different documents made available at the end of the 20th century show that DCI Dulles and associates went before the full CIA Subcommittees of the House Armed Services and Appropriations Committees to tell them what the Agency was prepared to do in the coming weeks. Although the documents show only a little of what transpired in the secret hearings, it is clear that some questions of the feasibility of the planned operation were raised; but there is no evidence that any legislator advised the Agency's leaders not to intervene in Cuba. The more significant point, however, is that the Subcommittees' members were told in advance of the Cuba plans. Russell and some other members on the Senate side were almost certainly told in advance, but no documentation seems to have been declassified regarding this.[11]

It is also clear that the practice of giving details about past and future covert actions did not begin in the Eisenhower or Kennedy era. Documents from the Truman era are less plentiful, but some of them support memories of former Agency personnel that, for example, DCI Walter "Beetle" Smith occasionally gave detailed operational briefings to members of CIA subcommittees. On one occasion, when a legislator asked a vague question about operations around the world, Smith pulled out a list of all ongoing covert action programs and reviewed them with subcommittee members.[12]

In summary, in the sensitive area of covert action, CIA subcommittees had a fair amount of knowledge, resulting from some of the few hearings each subcommittee held each year. It is likely, however, that many (especially smaller) operations occurred without being highlighted to legislators.

Intelligence Estimates

The sharing of information with the subcommittees (and occasionally other congressional bodies) was considerable. More than anything else, what legislators of the early Cold War era wanted from CIA leaders was their estimates of political and other conditions in nations around the world, especially the Soviet Union. DCIs Hillenkoetter, Smith, Dulles, and McCone routinely gave spoken summaries of analyses that CIA and other agencies had created. On the one hand, with the exception of the Joint Committee on Atomic Energy (JCAE)—which had a legal right to intelligence estimates on nuclear topics—the CIA rarely, if ever, gave copies of National Intelligence Estimates to committees, subcommittees, or their members to keep beyond the time of hearings. On the other hand, the CIA routinely prepared special estimates for legislators to keep.

One of the most sensitive topics treated by intelligence estimates came in the late summer and early autumn of 1962, when news media outlets and certain legislators (especially Senator Kenneth Keating [R-NY]) claimed that the Soviet Union was placing medium- or intermediate-range nuclear-armed missiles in Cuba. These claims contradicted U.S. intelligence estimates that called such a Soviet move unlikely. On such a topic, CIA subcommittee heads—who could be quite trusting and deferential toward the Agency during quiet times—became all business. As Deputy Director of Central Intelligence (DDCI) Marshall Carter noted on September 26, 1962, he had talked to Leverett Saltonstall, the ranking Republican on the Senate Armed Services CIA subcommittee, about the growing Soviet militarization of Cuba. "He said that he and Senator Russell considered this a very important matter and would like to be kept currently advised of whatever developed in the way of hard intelligence."

Over the ensuing weeks, during what became the Cuban missile crisis, Agency heads bent over backward to keep subcommittee leaders informed about the CIA's knowledge. Indeed, within twenty-four hours of President Kennedy being informed that the Soviets had missiles in Cuba, Russell summoned a nervous Carter and legislative liaison John Warner to his office to hear the full story. The CIA men knew that Kennedy had directed that the intelligence on missile sites be kept absolutely secret. Just after Carter and Warner greeted the Senator, Russell was called to a telephone and informed by the President that the CIA had important news for him. The briefers' task had been made immeasurably easier by the President's phone call, which apparently resulted from an alert to the White House by McCone concerning Russell's request for the latest intelligence.[13]

Counterintelligence

At certain points in the early Cold War, some legislative bodies pushed the CIA to share information about counterintelligence problems and controversies. Besides the CIA subcommittees, in the early 1950s, Republican Senator Joseph McCarthy's Permanent Subcommittee on Investigations harassed DCIs Hillenkoetter and Dulles about various (and sometimes nonexistent) problems. Also the House Un-American Activities Committee (HUAC) had interactions with the Agency on alleged infiltration of Soviet spies and sympathizers into the U.S. government. Few records of CIA-HUAC encounters seem to exist, though a tense encounter at a 1952 public hearing between DCI Smith and members of HUAC can be seen (in retrospect) to show the Director choosing his words carefully to avoid any mention of the harm done to U.S. intelligence by British traitor Kim Philby (who, in reality worked for the Soviet Union). However, Smith offered to be much more forthcoming with the Committee in a private hearing.[14]

A decade later, HUAC was more aggressive than the House Armed Services CIA Subcommittee in investigating the defection of two employees of the National Security Agency (NSA) in 1960. While the latter Subcommittee conducted

a brief investigation accompanied by hearings, HUAC (under chairman Francis Walter [D-PA]) pursued the topic for two years and forced certain reforms in personnel hiring, training, and clearance procedures at the NSA.[15]

Domestic Involvements of the CIA

The sensitive topic that the Agency may have withheld from the CIA subcommittees and other congressional bodies was that of periodic involvement in matters at home in the United States. The Church Committee and other mid-1970s investigations showed that the CIA sometimes spied on American citizens (such as peace activists), tested drugs on unwitting citizens, and illegally opened letters being handled by the U.S. Post Office. There are virtually no records even hinting that the CIA ever informed any congressional bodies or members of these activities in the 1950s or early 1960s. However, because only a handful of (usually partial) transcripts of CIA subcommittee hearings survive or have been declassified, and even detailed notes of such meetings are not plentiful, it is possible that the Agency did inform certain legislators about such legally questionable activities.

THE "OTHER" COMMITTEES AND THE CIA

Nothing is clearer in the papers of President Dwight D. Eisenhower than his hostility toward congressional "meddling" in the affairs of the CIA. Eisenhower directed his anger not toward the little subcommittees on CIA, though; despite occasional differences with them, he trusted men like Russell, Saltonstall, and Vinson to be discreet and responsible in their interactions with the Agency. Eisenhower's fury—there is no better word to describe it—was over the actions of other legislative bodies, whose leaders sometimes successfully insisted on having CIA leaders testify at hearings. Besides the Permanent Investigations Subcommittee and the HUAC, those bodies included the following.

The Senate Foreign Relations Committee

A few years before J. William Fulbright (D-AR) famously assumed the chairmanship of the committee in 1959, Foreign Relations had begun requesting testimony by Dulles on the CIA's analyses of worldwide political conditions and on its occasional intelligence failures. The frequency of such events is not well documented for all years, but—despite the unhappiness of Eisenhower over such Agency appearances on Capitol Hill—Dulles testified four or five times before the Committee or one of its subcommittees in 1958 and three times in 1959. Among the topics that the committee had Dulles analyze in their presence were Soviet military capabilities, the chances for Tibet to resist occupation by

China, and the odds that Cuban leader Fidel Castro would turn out to be a communist.

Among the real or alleged intelligence failures committed by CIA that DCI Dulles had to discuss with the Foreign Relations Committee in 1956–60 were the Hungarian and Suez crises in 1956, the launch of *Sputnik* in 1957, the 1958 attacks on Vice President Nixon in Venezuela, the Iraqi coup that same year, and the U-2 incident in 1960. Although Dulles generally received high marks from Committee members, the Agency received many criticisms and warnings in those sessions.[16]

The Air Force and Preparedness Subcommittees of the Senate Armed Services Committee

In 1956–57 hearings, the Air Force Subcommittee, headed by Stuart Symington (D-MO), was permitted by Committee chair Richard Russell to examine charges and supposed "intelligence" showing that the Soviet Union was far ahead of the United States in bomber aircraft capabilities. Later, Russell designated the Preparedness Subcommittee, headed by Senator Lyndon Johnson (D-TX), to examine charges that the Soviets excelled in long-range missile capabilities in 1958–60. But Symington, a member of Johnson's Subcommittee, often outdid the Texan in publicizing and identifying himself with the missile "gap."

The discreet Russell had mixed feelings about Symington, but the gap controversies were too fierce to be ignored. While Russell's own CIA Subcommittee could and did discuss the issues with Dulles and other Agency leaders, the Georgia Senator insisted that such hearings be kept secret. Thus, Symington's and Johnson's hearings, though held in "executive" (that is, secret) sessions, were much discussed in the press. Both senators readily discussed the hearings with journalists.

In testimony before the Air Force and Preparedness Subcommittees, Dulles denied Symington's charges that the Eisenhower administration had somehow misused intelligence or that the CIA itself had seriously underestimated Soviet military capabilities. The President himself responded in a 1960 press conference to Symington's charges that the administration had distorted intelligence as a means to reduce the size of the U.S. defense budget. In the words of a *New York Times* reporter, Eisenhower "appeared to control himself with effort." Such charges were "despicable," said the President, who added, "If anybody—anybody!—believes that I have deliberately misled the American people, I'd like to tell him to his face what I think about him." There was little doubt in anyone's mind about the identity of "him." Eisenhower was almost as angry, in private, against Dulles for "giving such detailed figures to the Congress."[17]

The Joint Committee on Atomic Energy

No committee of Congress angered Eisenhower more for its insistence on obtaining CIA estimates and testimony (on nuclear weapons topics) than the

JCAE. President Harry S Truman had been no fan of the Joint Committee either. On a good day, Truman might merely complain that "those fellows . . . think they are the board of directors" on atomic energy matters. When really angry (according to Atomic Energy Commission Chair David Lilienthal's diary), Truman "glared through his thickish glasses" and erupted over "those bastards on the Hill." Indeed, the JCAE was mandated by law to have full knowledge and substantial control over nuclear policies. In 1949, after the CIA failed to predict that the Soviet Union would conduct a successful test explosion of its first atomic bomb, the Joint Committee virtually skinned alive DCI Hillenkoetter in a secret hearing. In the 1950s, Dulles's usual responsiveness to JCAE requests for information and testimony was a chronic irritant in the DCI's relationship with the White House.[18]

THE WAXING AND WANING OF OVERSIGHT

Records that have been declassified or otherwise made available in recent years show clearly that congressional oversight of the CIA varied from one year to the next. Why did the Agency appear before no more than a dozen hearings in 1955, but testify twice as often in 1958? There are two fairly obvious answers.

The Political Environment

In an influential 1984 article, political scientists Matthew McCubbins and Thomas Schwartz suggested that conditions in the American political environment largely determined whether Congress would aggressively investigate failures and wrongdoing by executive branch agencies or remain relatively passive and deferential toward them. As they point out, with the Legislative Reorganization Act of 1946, Congress mandated itself to engage in continuous, assertive oversight (what McCubbins and Schwartz called "police patrol" oversight). But the reality of the ensuing decades was that Capitol Hill became assertive only when "fire alarms" were set off by interest groups, the news media, the public, or others complaining that one or more agencies had somehow failed.[19]

On the whole, the fire alarms analysis fits well with the surviving evidence about Congress and the CIA in the early Cold War decades. An examination of the news in 1955 and 1958, for example, shows that there were many more alarms ringing in the latter year: a firestorm over *Sputnik*'s launch late in the previous year, Nixon's encounter with South American rioters, and the coup in Iraq. There was enormous critical news coverage of the CIA that year—more than in any previous year—as well as letters from citizens to newspapers, Congress, and the White House. After the year ended, an aide to Dulles reflected in a work diary on the "ground swell developing for more frequent briefings of these committees on some systematic basis."[20]

Attributes of Legislators

Much as the level of controversy in the American political environment affected the amount of congressional oversight of CIA, there can be no doubt that attributes of the legislators charged with carrying out such duties mattered, too. Consider the different approaches to CIA used by Representative John Taber (R-NY) and Senator Carl Hayden (D-AZ).

Taber chaired the House Appropriations Committee and its CIA Subcommittee during the two first years of the Eisenhower presidency, when the Republican Party held a majority of seats in Congress. By all accounts, he was not a likable man and had no real friends in the House, but he was tough and capable. As chair, Taber hired new staff to examine the budgets of the CIA and many other bureaucracies. The Subcommittee held more hearings annually with the CIA than had ever been the case. He obtained more detailed descriptions of CIA successes and failures in covert action than apparently had been given by Agency heads before. He placed limitations on both spending and new hires at the Agency, provoking widespread complaints there. A new verb joined the Washington lexicon—to *taberize* was to cut budgets. After Democrats regained control of Congress, Taber continued to show an active interest in CIA affairs.[21]

Hayden was genuinely popular and respected in the Senate, but by the time he assumed the chair of its Appropriations Committee in 1955, he was seventy-seven years old. Though bright and hard-working, Hayden was overly busy. He had high regard for Richard Russell, the most senior of his colleagues on Appropriations. Since Russell chaired Armed Services and its CIA Subcommittee, Hayden and he agreed some time around 1956 that they would combine their subcommittees' oversight of CIA, under Russell's leadership. Although this could have led to reasonably effective monitoring of the Agency, it did not, at least concerning budgetary matters. Hayden was the least effective of any heads of CIA subcommittees in the 1950s.

Scrutiny of proposed CIA budgets was far greater in the House, where Clarence Cannon (D-MO) chaired Appropriations from 1955 through his death in 1964. Cannon has been criticized in histories of the CIA as essentially an old fool who did no more oversight than to trade stories with Dulles and McCone and ask them if the CIA had "enough" money. The reality was different. For example, before anyone else in Washington, Cannon insisted in 1958 that Dulles answer a simple question: "How much does the United States government spend annually on intelligence activities?" Theoretically, a Director of Central Intelligence managed the entire American intelligence establishment, but the reality was that agencies other than the CIA received almost no direction from Dulles or other early DCIs. It took months of work by the CIA and other agencies before Dulles could give Cannon a reasonably accurate response in 1958. They would have to give a fuller report the following year.[22]

Among the other legislators who interacted with the Agency, there were many who—even if respectful toward CIA—were reasonably assertive, especially

when alarms were going off. These included in the Senate: Symington, Bridges, John Stennis (D-MS), and Kenneth McKellar (D-TN). In the House, Francis Walter, chair of HUAC, was a periodic thorn in the side of Dulles. The two men actually argued in one telephone conversation, with the chairman hanging up on the DCI.[23] Also in the House, starting around 1957, Clarence Cannon appointed the widely respected George Mahon (D-TX) to head the Appropriations CIA Subcommittee. Cannon remained periodically active in relation to CIA, but Mahon took more of the burden and stepped up the frequency and substance of hearings.

Similarly, Carl Vinson appointed the well-regarded Paul Kilday (D-TX) to head the Armed Services CIA Subcommittee and improve its work. Among other things, Kilday oversaw very secretive investigations of the CIA in 1959 and the NSA in 1960. Kilday attempted to increase examinations of the CIA's budget by the General Accounting Office (GAO), an arm of Congress. Vinson had long relied on Kilday for assistance on crucial work, but on the GAO issue, Vinson withdrew his support of Kilday and the idea died.

Kilday believed that the appropriate subcommittees of Congress should monitor intelligence agencies, but Vinson wavered on this point. After Kilday retired in 1961, Vinson resumed chairing the Armed Services Subcommittee and actually told DCI McCone at the beginning of 1962 that "it was not necessary that the Subcommittee know everything concerning Agency affairs." (In fairness to Vinson, records show that when Congress was in session, his Subcommittee held hearings with CIA witnesses almost monthly in 1962 and 1963, and discussed topics that Agency censors were still "sanitizing" from documents released early in the 21st century.)[24]

Others in the House and Senate displayed the sort of deference that Vinson voiced. Saltonstall, the ranking Republican on Senate Armed Services, had such faith in Dulles and McCone—both actual friends of the Senator—that he seems to have only rarely pushed hard for information about the CIA.

In summary, although it is fair to say that congressional oversight of the CIA generally increased across the years from 1947 through 1963, the trend was not steady. In years when events seemed less threatening to U.S. national security, oversight was likely to decrease. Still, the rise and fall of oversight depended, too, on the attributes of those legislators on the CIA subcommittees or elsewhere in Congress.

TWO DEBATES ABOUT CIA'S ACCOUNTABILITY

On the floors of the House and Senate, members only occasionally discussed the CIA. When they did, it was usually because of some surprise in world politics. Occasionally, though, the Agency's place in the U.S. political system was the topic. Two of the most substantive debates about whether or not it was subject to direction from constitutionally elected leaders occurred in 1956, when Senator

Mike Mansfield (D-MT) offered a resolution to create a joint congressional committee on intelligence, and in 1962, when the Senate debated President Kennedy's nomination of John McCone to become DCI.

The Mansfield Resolution

Mike Mansfield was an atypical politician—not a back-slapper, not long-winded, and not especially egotistical. He cared and thought about democratic governance. Though an early supporter in the House of the CIA, after entering the Senate in 1953, Mansfield came to believe that the Agency was free from reasonable controls by the White House and Congress. He could do little to make Presidents give more attention to the Agency, but Congress (he thought) should become far more active in monitoring the CIA and other intelligence agencies.

The Montanan had been promoting his resolution since 1953. By early 1956, he had won many supporters, including a bipartisan majority of the members on the Armed Services Committee. In April debates, Mansfield said that everything about the Agency was "clothed in secrecy," and that this invited "abuse." Furthermore, it seemed likely that "all is not well with CIA," in light of reports that Congress suffered from "a woeful shortage of information about the CIA."

On the first day of debate, the main defender of the existing oversight system was Leverett Saltonstall. The Massachusetts Senator stumbled badly in that role, though, speaking of the "difficulty in connection with asking questions and obtaining information . . . which I personally would rather not have, unless it was essential for me, as a Member of Congress, to have it." He had not said that he did not obtain sensitive information, but that was the impression he left.

Two days later, Richard Russell tried to make up for Saltonstall's weak defense. His CIA Subcommittee had asked Dulles "very searching questions about some activities which it almost chills the marrow of a man to hear about." Russell even claimed that the CIA faced more congressional oversight than most other government agencies. In light of that assertion, his pledge about the future may not have signified much: "I shall undertake to exercise as close supervision over this Agency as is ordinarily exercised by parent committees of the Congress in dealing with agencies which are responsible to them."

Mansfield was not helped by allies. Wayne Morse (D-OR) charged Saltonstall with supporting an "American police state system." Joseph McCarthy spoke of incompetence and communist infiltration at CIA and complimented "the able senator from Montana," but the once fearsome McCarthy was in the late stages of alcoholism—"a piteous specter with a bloated face" that day, noted a Senate observer.[25]

Some senators who implied that the CIA needed more oversight were not willing to vote for it. One defended his surprising vote with the claim that to establish an intelligence committee with a significant staff, would "dry up sources of information."

Though the debate over CIA's functioning in a democratic system was notable, it probably had nothing to do with the outcome. Russell and his ally, Majority Leader Lyndon Johnson, marshaled votes, with an assist from the White House and Allen Dulles, and fifty-nine senators voted "no." The CIA subcommittees, with periodic assists from other congressional bodies would—for better or worse—continue to be the system by which Congress monitored the Agency's performance.[26]

The McCone Confirmation Debate

When prior DCIs were nominated by Presidents Truman and Eisenhower, Senate debates were perfunctory and the voice votes unanimously favorable. When President Kennedy nominated Republican John McCone, a businessman who had served the two most recent Presidents (among other things, heading the Atomic Energy Commission), it provoked serious debate and actual opposition. Part of this was a result of McCone's longtime substantial holdings in corporations that had major contracts with the United States or foreign governments, and part derived from his lack of direct experience in intelligence. But the nomination was also hostage to a serious conviction in the Senate that as Eugene McCarthy (D-MN) said, "There is no regular or normal procedure . . . by which committees of the Congress are consulted or informed of CIA activities." Sooner or later, the question of proper congressional oversight of the Agency and its questionable operations "will have to be the basis for a great debate. I think this is the proper time to start that debate."

Most disappointing to the Kennedy administration was the decision of Senator Fulbright to join McCarthy's fight against McCone. Fulbright said he could have voted for McCone as Secretary of State, for that position was subject to "constant review and exposure to criticism." A DCI clearly influenced policy making, Fulbright claimed, but McCone had not been required to state his policy views when he had testified before the Armed Services Committee days before. In the face of assertions by CIA/McCone supporters that the Agency did not have a major influence over U.S. foreign policy, the Foreign Relations chair stated bluntly that this was "not in accord with the facts as I know them."

Senator Russell was horrified "that we air on the floor of the Senate all the things that CIA is reputed to have done or not to have done in foreign countries." He avoided saying that CIA Subcommittee members often had specific knowledge of such things, but claimed, "No Director of Central Intelligence would think of undertaking any activities anywhere on the face of the earth without the approval and consent of the President." Furthermore, there had been "six or seven hearings" before the Senate Armed Services and Appropriations Subcommittees in 1961, so Fulbright's charge that the CIA was not accountable to Congress was inaccurate. Fulbright's real complaint (Russell charged) must be that "it is not all under his Committee."[27]

The fierceness of the opponents to the confirmation before and during the debates actually unnerved the usually tough McCone. While traveling abroad as director-designate, he wondered (in a wire to his associates at the CIA) if it would be best if his nomination were withdrawn. John Warner and a colleague cabled back, "The President retains fullest confidence in you. . . . We believe it unnecessary and undesirable to even consider withdrawal." An "overwhelming affirmative" vote was likely, they said, and they were correct. The vote was seventy-one to twelve. As the *New York Times* noted, though, that numerical tally obscured the considerable "uneasiness about the agency's freedom from congressional supervision." Many of McCone's supporters were like Mike Mansfield, by then the Majority Leader in the Senate: they voted for the new DCI mostly out of loyalty to the President.[28]

CIA AND DEMOCRATIC ACCOUNTABILITY, 1947–63

Was the CIA responsive to constitutionally elected leaders in the Truman-to-Kennedy era? While CIA–White House relations are not the focus of this chapter, it is worth pointing out that the weight of scholarship in recent decades has suggested that rather than being a "rogue elephant," the CIA was substantially a tool of the White House.[29] What about Congress? Numerous documents from the CIA and Capitol Hill have only become available recently, after many decades with very little publicly available evidence to go on. In those years, there was no possibility of a large body of literature on CIA's accountability to Congress. Even now, so much remains classified—or was destroyed or never committed to paper—that it is entirely possible we will never have a truly detailed documentary record of CIA-Congress interactions in the early Cold War decades.

Based on what has become available, however, a better debate can take place over who was right: Senators Mike Mansfield and Eugene McCarthy or Senators Richard Russell and Leverett Saltonstall? Was CIA mostly free from accountability to anyone in Congress, as Mansfield and McCarthy charged, or did a select number of legislators usually know of bone-chilling Agency activities?

I argue that neither of those two stances was quite right. There were far more Agency appearances on Capitol Hill and many more descriptions of sensitive activities to the CIA subcommittees than Mansfield or McCarthy knew. Any future scholarly treatment of the CIA's democratic accountability in the early Cold War must take into account, especially, the documentary record of Allen Dulles's and John McCone's substantial time on Capitol Hill.

Regarding covert action, perhaps the most controversial realm in which the CIA was active, there is now substantial evidence to negate Mansfield's suggestions that such operations were done without knowledge or support on Capitol Hill.

There were even a few congressional investigations of the CIA: by Taber in 1953, Joseph McCarthy in the early 1950s, Kilday in 1959, and Stennis in 1963.

There may have been others. Also, investigations headed by Johnson, Symington, and some others touched partly on the CIA.

To the extent that the subcommittees did not know of certain morally or legally questionable activities, though, it appears that the legislators were as much to blame as Agency leaders. Clearly, sometimes people like Vinson or Saltonstall did not want the subcommittees to know the CIA's darkest secrets, and they may have chosen not to hear them either in hearings or in private.

However, the available records hardly suggest support for Richard Russell's claim that the CIA was more extensively monitored that most other bureaucracies of the executive branch. In a typical year, each subcommittee on the CIA met with Agency leaders a few times. The leaders of those subcommittees were busy heading other important congressional bodies; and the staffers who assisted those subcommittee leaders always had to divide their time between work on CIA matters and that of other agencies such as the Department of Defense. It may be revisionist to suggest that oversight of some real substance occurred in the early Cold War years, but it would be bizarre to claim that such oversight was systematic or comprehensive.

NOTES

1. William Leary, ed., *The Central Intelligence Agency: History and Documents* (Tuscaloosa: University of Alabama Press, 1984), pp. 143–45.

2. Harry Howe Ransom, *Central Intelligence and National Security* (Cambridge, MA: Harvard University Press, 1958), p. 145.

3. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Book 1: Foreign and Military Intelligence,* p. 150.

4. David M. Barrett, *The CIA and Congress: The Untold Story from Truman to Kennedy* (Lawrence: University Press of Kansas, 2005), p. 174. Papers of over two dozen legislators who interacted with CIA from 1947 to 1960—used in writing this chapter—are available in the David M. Barrett Research Files at the Richard Russell Library, University of Georgia.

5. Barrett, *CIA and Congress,* p. 321, has brief treatment of numbers for autumn 1957 through autumn 1958. Specific documents on 1958 can be found in that year's folders of the Barrett Research Files at the Russell Library.

6. Barrett, *CIA and Congress,* chaps. 27–29.

7. McCone, "Meeting Attended by the President . . . ," October 9, 1962, *Foreign Relations of the United States: Cuba, 1961–63,* vols. 10–12, microfiche. The memo closes with a description of the private LBJ-McCone meeting. A good example of a DCI's adherence to directives is in McCone, Memo for File, August 21, 1962, in Mary McAuliffe, *CIA Documents on the Cuban Missile Crisis* (Washington: CIA, 1992), p. 21.

8. Barrett, *CIA and Congress,* chap. 3. In one or two of those earliest years, it may have been only the chair of House Appropriations who knew budget details.

9. Stephen Horn, *Unused Power: The Work of the Senate Committee on Appropriations* (Washington, DC: Brookings, 1970). Horn's book features rare, early treatment of a CIA subcommittee; see pp. 38–40, 76, 97–100, 127, 135, 178, 186.

10. Barrett, *CIA and Congress*, pp. 96, 103–12.

11. Barrett, *CIA and Congress,* pp. 438–46; Jack Pfeiffer, *Official History of the Bay of Pigs Operation,* vol. 3, pp. 194–95, CIA Miscellaneous Records, Box 1, JFK Assassination Records Collection, National Archives.

12. Interview with Walter Pforzheimer (CIA's first legislative liaison), September 30, 1994, Washington, DC.

13. Interview with John Warner, October 19, 1999, Washington, DC; Carter, memo for the record, September 26, 1962, CREST (CIA Records Search Tool), National Archives, College Park, MD; M. Bundy to President Kennedy (re: Russell request), October 17, 1962, document no. 654, Cuban Missile Crisis collection, National Security Archive, Washington, DC.

14. Barrett, *CIA and Congress,* pp. 127–34.

15. Ibid., p. 421; James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency* (Boston: Houghton Mifflin, 1982), pp. 81–85, 147–50.

16. Barrett, *CIA and Congress,* chaps. 25–29, 34, 39.

17. Ibid., pp. 367, 369–70.

18. Ibid., pp. 51, 56–62, 142, 209, 322.

19. Matthew McCubbins and Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms," *American Journal of Political Science* 28 (1984), pp. 165–79.

20. L. K. White, diary, February 4, 1959, quoted in Barrett, *CIA and Congress,* p. 322.

21. Barrett, *CIA and Congress,* chap. 15.

22. Ibid., pp. 317–18.

23. Ibid., p. 421.

24. Warner, memo for the record (Vinson), January 16, 1962, CREST. On Kilday, see Barrett, *CIA and Congress,* pp. 334–39, 391–92, 440–46; on Mahon, Barrett, *CIA and Congress,* pp. 121–22, 296–97, 341–46, 453–55.

25. Richard Riedel, *Halls of the Mighty: My 47 Years at the Senate* (Washington: Robert B. Luce, 1969), p. 229.

26. Barrett, *CIA and Congress,* pp. 223–33; *Congressional Record,* April 9 and April 11, 1956, pp. 5891–939, 6048–68.

27. *Congressional Record,* January 29, January 30, and January 31, 1962. Quotations are from lengthy memoranda prepared by CIA personnel for McCone, obtained from CREST.

28. [Name censored] and Warner to McCone, undated (from late January 1962), CREST; *New York Times,* February 1, 1962, p. 9.

29. See, for example, Christopher Andrew, *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush* (New York: Harper Collins, 1995); Thomas Powers, *The Man Who Kept the Secrets: Richard Helms and the CIA* (New York: Knopf, 1979); and Don Bohning, *The Castro Obsession: U.S. Covert Operations Against Cuba, 1959–1965* (Washington: Potomac Books, 2005). Despite the Church Committee's view that congressional oversight of CIA was severely lacking, it did not endorse the "rogue elephant" analogy.

2

INTELLIGENCE OVERSIGHT

The Church Committee

FREDERICK A. O. SCHWARZ JR.

THIRTY YEARS AGO, THE CHURCH COMMITTEE COMPLETED what was and still is the most exhaustive look at our government's (or any government's) secret intelligence agencies. The Committee's hearings and reports to the U.S. Senate and to the American public revealed much that broke America's laws and did not honor America's values.[1]

Not knowing a single senator, I was honored to be asked, and privileged to serve, as the Committee's chief counsel. Now, thirty years later, when America again faces and fears a ruthless enemy, I am frequently asked about the Church Committee and whether its lessons are important in a time of terror. They are. Most important, in its extensive review of excess and abuse over the course of approximately thirty years during the Cold War, the Church Committee showed that in times of crisis, even constitutional democracies are likely to violate their laws and forget their values. This was a lesson as old as the Alien and Sedition Acts and as recent as the internment of Japanese Americans during World War II. But the Church Committee analyzed the toxic elements of secrecy and the extensions of a climate of fear for decades instead of the shorter periods involved in the earlier periods of excess. The danger signals raised by an indefinite war on terror are obvious. Whether an oversight committee can make a difference is affected to a considerable extent by whether it and the country it serves is overly partisan or not. In 1975–76, the climate was far less partisan than today. Although there were some differences among Church Committee members, these were not major, focusing mainly on details of recommendations and whether some material should be made public (e.g., the Assassinations Report, or the names of companies that turned over all their cables to the National Security Agency [NSA]). These differences were not partisan, and the Committee never divided on partisan lines.

The less toxic atmosphere of the day helped. And so did the Committee's willingness to expose facts concerning—and criticize icons of—both parties.

Today, public comment looking back tends to identify Cold War abuses with the Nixon years, or even just Watergate. This hides more than it explains. Richard M. Nixon makes a convenient larger-than-life villain. But as revealed by the Church Committee, no single man, no single administration, no single party caused the abuses and overreaching of the Cold War period. In fact, overly broad investigations, lawless conduct, and a departure from America's ideals haunted all administrations from Franklin D. Roosevelt through Nixon.[2]

Lack of congressional oversight was one of the causes of these failures. This lack, coupled with excessive secrecy and the use of fuzzy standards in administrative directives, and sometimes in the laws themselves, was the fertilizer for abuse and excess.

Today, compared with the era of the Church Committee, not only are we more partisan as a nation and in government, but the problem of oversight during the war on terror is that oversight must necessarily be of a sitting administration. This makes it much harder. Nonetheless, principles that the current administration has advocated—such as that presidents are above the law—raise concerns that our founders understood and guarded against and create precedents that are dangerous in the hands of a president of any party. So the question is whether those who are responsible for oversight have the wisdom and the courage to rise above the moment and together take a long term, nonpartisan view of what best serves our country.

CREATING THE COMMITTEE

On January 27, 1975, the U.S. Senate created a Select Committee to investigate the intelligence agencies of the United States, including the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA). The Committee's mandate was to investigate the full range of government intelligence activities. The two most basic questions were (1) the extent to which the agencies' actions had been "illegal, improper or unethical," and (2) oversight: "the nature and extent of executive branch oversight" and the "need for improvement" of congressional oversight.[3] The Committee became known as the Church Committee for its chair, Idaho's Frank Church (D), elected nineteen years earlier at the age of thirty-two.

The Committee issued its final reports in April 1976. Here are just two examples of the disclosures. First, internal FBI documents used Orwellian language to label Martin Luther King Jr. the leader of a "Black Nationalist *Hate* Group." Then the Bureau set out secretly to destroy King, including sending an anonymous letter with an enclosed tape that appeared to be designed to induce him to commit suicide.[4] A second revelation was the years of CIA assassination plots, including the hiring of Mafia members to try to kill Fidel Castro.[5]

Other examples of intelligence agency misconduct are mentioned below. Beyond exposure of agency misconduct, the Committee highlighted grave deficiencies of presidents, attorneys general, and other high executive branch officials. The same went for Congress.

HOW DID THE INVESTIGATION HAPPEN?

Powerful, secretive intelligence agencies do not like their dirty laundry exposed. Presidents do not want executive branch responsibility examined. Congress traditionally had shied away from its intelligence oversight responsibilities. Why, then, in 1975 did the Senate—and later the House—launch major investigations of the intelligence agencies?

For the investigation to happen, pent-up interest in what America's hidden government had been doing was necessary. There had been rumors of assassination plots. A break-in to an FBI office in Pennsylvania had found documents suggesting secret harassment of dissidents. And finally, in December 1974, Seymour Hersh wrote a series of *New York Times* articles exposing "massive" CIA domestic spying and illegal intelligence operations directed against antiwar activists and other American dissidents.[6]

Coupled with interest in what our secret government had been doing was increased public mistrust of government. This stemmed from the Vietnam War and Watergate. Many senators and members of Congress also worried about their country and about the balance of power between the executive and legislative branches.

But while the interest and the increased mistrust were *necessary* for the investigation, neither would have been *sufficient* to unleash or allow the Church Committee investigation. Three factors helped.

First, Gerald R. Ford had recently become our first unelected president. He had pardoned Richard Nixon. Having taken over from a man discredited and disgraced for violating the law and abusing his power—including attempting to coopt the CIA and the FBI—President Ford had a problem. On the one hand, he wanted to appear open or, perhaps more important, did not want to appear to be hiding impropriety. On the other hand, powerful advisors like Henry Kissinger opposed any meaningful cooperation. Ford had to be pushed—repeatedly—to allow the Committee access to the crucial raw files and relevant witnesses. Nonetheless, ultimately he chose not to face a public fight with the Senate committee over access.[7]

Second, after directing the FBI for almost fifty years, J. Edgar Hoover was dead. With good reason, public officials feared Hoover, as well as the general public's reverence for the FBI. The Church Committee came across a striking example of Hoover's power. After understanding the colorful details of the Castro assassination plots (and others), the crucial question became whether Presidents Eisenhower, Kennedy, and Johnson had authorized the plans. In the case of

Kennedy, the Committee uncovered the fact that a mistress of the Mafia don hired by the CIA to kill Castro was at the same time one of JFK's mistresses. Was she a go between? We concluded no. But in the course of examining this case, we came upon a letter from Hoover to the White House and Attorney General Robert Kennedy that revealed that Hoover knew about the joint mistress.[8] After this, it surely would have been difficult for President Kennedy or his brother to replace Hoover or even effectively control him. Similarly, it seems unlikely that with Hoover alive, Congress would have unleashed a major investigation of the FBI.

Third, in contrast to today's Congress—where partisan diatribes chill debate and make wise action more difficult—Congress was then more collegial. Evidence was the decision by Majority Leader Mike Mansfield (D-MT) that the Select Committee's membership be six Democrats to five Republicans, at a time when regular committees were divided more favorably to the Democrats. It is also possible that some senators assumed revelations of presidential misconduct would be limited to the already disgraced Nixon. As it turned out, however, one of the Committee's most important contributions was to show that all presidents, starting with FDR, had failed in their duty to supervise the secret government. Moreover, most had themselves been complicit in abuse.

AT HOME AND ABROAD: THE COMMITTEE'S DUAL FOCUS

The Church Committee covered domestic and foreign issues, as indicated by the titles of its main reports: *Alleged Assassination Plots Involving Foreign Leaders,* an Interim Report; *Foreign and Military Intelligence, Final Report Book I*; *Intelligence Activities and the Rights of Americans, Final Report Book II*; and *Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Final Report Book III*. There were, of course, many common themes and questions. Had excessive secrecy facilitated abuse and caused mistakes harmful to the national interest? The same question was asked with respect to vague, ambiguous, or open-ended authorizing language voiced by presidents or contained in statutes. Had the executive branch exercised proper control? Did Congress have appropriate oversight? Had the programs and policies served the national interest? Finally, the most fundamental question: Should the United States, when faced with crisis, react by adopting "the tactics of the enemy?" In addition, the evidence, particularly as developed in questions by Senator Walter "Fritz" Mondale (D-MN), who led the work focused on the rights of Americans, showed that attitudes developed in foreign intelligence operations seeped through at home. Thus, disregard for the "niceties of law" was "brought home" from war by some of the FBI officials who were responsible for examples of despicable conduct at home, including the effort to destroy Dr. King.[9]

Despite the similarities, there were also fundamental differences between the Committee's approach to domestic and foreign issues. This is partially explained

by the different standards applicable to intelligence activities affecting the rights of Americans, as opposed to intelligence activities overseas. To simplify, the former can be held to the U.S. Constitution, the Bill of Rights, and the majesty of the law. But the latter can best be held to the more general early words of the Declaration of Independence: "a decent respect to the opinions of mankind." In addition, reflecting a number of factors, the reports other than Book I were based on the supposition that detailed facts drive reform and thus were more fact-based and reflective of investigation. In contrast, Book I was more policy-oriented. Loch K. Johnson's book, *A Season of Inquiry* discusses the differences in approach in more detail.[10]

THE INGREDIENTS OF SUCCESSFUL OVERSIGHT

Frank Smist, in his book *Congress Oversees the United States Intelligence Community, 1947–1989,* divided *oversight* into two categories: "institutional" and "investigative." The institutional model sees oversight as a "cooperative relationship between the legislative and executive branches." The investigative model views oversight as involving an "adversarial relationship" between the two branches.[11] Of all the congressional committees responsible for intelligence oversight from 1947 through 1989 reviewed by Smist, the Church Committee was the only one characterized as "Investigative and Institutional Oversight Combined."[12] Oversight by the permanent Intelligence Committees created after the Church Committee are, generally speaking, examples of institutional oversight.

Recognizing the limits of my experience, I nonetheless tender five elements needed for successful oversight: a historical perspective; delving deeply and comprehensively into the facts; handling secrecy sensitively; having empathy for but also maintaining distance from the agencies; and being nonpartisan and sharing core values. (Discussion of the first four elements follows immediately; the last is discussed in the section on values.)

The Need to Understand History

One of the Church Committee's tasks was to assess how well our government had balanced liberty and national security during a time of crisis—the Cold War, roughly a 40-year period. What happened during earlier crises was also instructive. There was a pattern of overreaching, including the Alien and Sedition Acts at the dawn of our Constitution, the Palmer Raids after World War I, and the internment of Japanese Americans in World War II. The Cold War period was different from these in two respects: first, the crisis was much longer; and second, unlike the earlier periods, most of what the government did was secret. For the Church Committee to fulfill its mandate, it had to understand both the similarities to and the differences from the earlier eras.

In addition to remembering episodes from much earlier time, it was valuable to understand the historical origins of the programs reviewed by the Committee.

For example, consider how the FBI went from investigating possible criminal conduct to enormously broad spying on Americans who had done nothing to threaten their country. This, too, required a look at history.[13]

Harlan Fiske Stone was appointed attorney general by President Calvin Coolidge in 1924. Later he described the conduct of the Justice Department and the Bureau of Investigation (the original name of the FBI) before he took office, as "lawless, maintaining many activities which were without any authority in federal statutes and engaging in many practices which were brutal and tyrannical in the extreme." Shortly after taking office, Stone set a new standard for the Bureau. He warned that "a secret police may become a menace to free government and free institutions, because it carries with it the possibility of abuses of power that are not always quickly appreciated or understood." He then announced that the Bureau "is not concerned with political or other opinions of individuals. It is concerned only with their conduct and then only such conduct as is forbidden by the laws of the United States."[14]

Stone cleaned house and—with the support of the American Civil Liberties Union (ACLU)—promoted J. Edgar Hoover to direct the Bureau. Eight years later, Hoover was still marching to Stone's drum, telling Congress that because the Bureau was subject to "the closest scrutiny," it should not investigate matters which "from a federal standpoint, have not been declared illegal."[15]

But then, leading up to World War II, President Franklin Roosevelt issued a series of conflicting and confusing directives to Hoover. Some were consistent with the Stone standard, referring to investigation of conduct "forbidden by the laws of the United States" such as espionage, sabotage, and violations of the neutrality regulations. Others added the loose term "subversion." The President, Attorney General Homer Cummings, and Hoover explicitly decided not to seek legislation about their plans for expanded domestic intelligence; "in order to avoid criticism or objections," the plans "should be held in the strictest confidence," not even revealed to Congress.[16]

What was actually done during the Roosevelt years usually was appropriate investigation of possible criminal conduct by Nazis or Nazi sympathizers. But the Bureau did, on occasion, investigate perfectly lawful conduct of entirely legal groups such as the League for Fair Play, formed, according to the Bureau, by "two ministers and a businessman for the purpose of furthering fair play, tolerance, adherence to the Constitution, democracy . . . and good will among all creeds, races and classes." The FBI also started a decades-long infiltration of the National Association for the Advancement of Colored People (NAACP), even though it was clear from the outset that its purposes were entirely lawful. And at the Roosevelt White House's request, the Bureau opened files on all who had sent telegrams to the White House expressing approval of a speech by Charles Lindbergh, one of the President's leading critics.[17] Still, what was most important about the Roosevelt era was that the vague word subversion, and the decision to keep secret the fundamental change in approach planted seeds for the abuses highlighted by the Church Committee.

The Importance of Facts

Without facts, oversight will be empty. Moreover, the facts must be detailed and cover a wide range. Only with that kind of record can one or be sure one understands patterns or be confident of conclusions.

An Emotional High Point: Senator Phillip Hart Shows How Facts Can Change Minds

On November 18, 1975, the Committee began its public hearings on the FBI. Reflecting the Committee's bipartisan approach, Senator Church and Vice Chairman John Tower (R-TX) opened the hearings by stressing the importance of "periodic public scrutiny" (Church) and "establishing a complete and open record" (Tower).[18] Further demonstrating the bipartisan nature of the inquiry, the hearing started with Chief Counsel Schwarz and Minority Counsel Curtis Smothers jointly providing a lengthy opening presentation of evidence and what it showed about the Bureau, presidents, and attorneys general.[19]

After counsel provided a detailed and disturbing litany of lawlessness, Chairman Church turned to questions and comments from senators, first recognizing Michigan's Senator Phillip Hart (D). Church expressed pleasure at Hart's return after "some weeks of absence." What Church did not say—but everyone knew—was that Hart had been away being treated for the cancer that killed him the next year.

Noting that he did not "recommend that others pursue the course I took to get this advantage" of commenting first, Hart began by telling how he had for years rejected claims of FBI impropriety: "As I'm sure others have, I have been told for years by, among others, some of my own family, that this is exactly what the Bureau was doing all of the time, and in my great wisdom and high office, I assured them that they were—it just wasn't true. It couldn't happen. They wouldn't do it." Then Hart described how the facts recounted by counsel had changed his mind and set out the two broad challenges facing the Committee:

> What you have described is a series of illegal actions intended squarely to deny first amendment rights to some Americans. That is what my children have told me was going on.
>
> The trick now, as I see it, Mr. Chairman, is for this Committee to be able to figure out how to persuade the people of this country that indeed it did go on. And how shall we insure that it will never happen again? But it will happen repeatedly unless we can bring ourselves to understand and accept that it did go on.[20]

Johnson's book about the Committee describes this as an "emotional high point"—Hart's weakened voice, tears in the eyes of staffers, and "in the opinion of many observers, the Committee's finest moment."[21]

Access to Facts and Witnesses

But of course, there can be no mind changing unless one has the facts.

Reports about the facts by the government agency itself are often useful but seldom sufficient. A good example of where internal reports can be insufficient, indeed misleading, arose in the Committee's investigation of the FBI's Counterintelligence Program (COINTELPRO)—"an ugly little acronym which would have been at home in any police state."[22] After hints about COINTELPRO appeared, Attorney General William B. Saxbe asked for an internal report. Revealingly, even though the Bureau was part of the Justice Department, it resisted letting the Attorney General's office see the COINTELPRO files, claiming that to do so would jeopardize national security. Instead, the Bureau said it would summarize the facts of each COINTELPRO action. These summaries were often extremely misleading. For example, one described a letter, purporting to come from the Chicago Black Panthers, that was sent by the FBI to the leader of the Blackstone Rangers, a "black extremist organization in Chicago." The Bureau's summary described the letter's purpose as to "hopefully drive a wedge between" the two groups. The actual letter, however, said the Panthers had "a hit out" for the Rangers' leader. And the actual cover memo that supported sending the letter said that the Rangers were prone to "violent type activity, shooting and the like." The cover memo predicted the letter may lead to "reprisals" against the Panthers' leadership.[23]

Development of a serious factual record also requires access to the actual contemporaneous documents and to witnesses, at both high and low levels. On this, the CIA proposed that an agency monitor should accompany any current or former intelligence official called in for questioning, including preliminary questioning by staff. In addition to observing, the monitors could give the witness "advice." Again showing the Committee's bipartisan approach, Senator Richard Schweiker (R-PA) said if this were allowed, "we'd be the laughing stock of the Hill," and Vice Chair Tower made the motion leading to a unanimous vote to reject.[24] Witnesses thereafter always appeared untethered.

Handling Secrecy Sensitively

Investigating secret government programs requires access to secrets. It forces analysis of the overuse of secrecy stamps and of the harm caused by excessive secrecy. Ultimately, it may require describing and revealing secrets. Nonetheless, obviously there are legitimate secrets. Oversight or an investigation that is heedless of that is doomed, as well as irresponsible.

The Church Committee worked out reasonable arrangements with the agencies and the White House. There were two key agreements. First, when the agencies were producing documents, they could, in the first instance, redact—or black out—the names of informers (not agents). Thus, the Committee would learn about the fact of FBI infiltration of the NAACP or what the FBI called the

Women's Liberation Movement and see the reports of the informers, without getting the informer's name. Then, if the Committee felt it was important to have the name, it would press for it. Second, the Committee agreed that before it issued its reports, it would let agencies see them to be able to argue that more details were being released than necessary or appropriate.

The Committee's reports are enormously detailed. They reveal much information that had been secret. No improprieties were withheld. But sensible limits were placed on the details disclosed. For example, the actual names of lower-level undercover agents who had been tasked by bosses to do unseemly or illegal acts were not used in the reports; the bosses's names, however, were included. Another example is shown by the introduction to the Staff Report on Covert Action in Chile, 1963–75, which noted that: "With few exceptions, names of Chileans and of Chilean institutions have been omitted in order to avoid revealing intelligence sources and methods and to limit needless harm to individual Chileans who cooperated with the Central Intelligence Agency."[25] These sensible agreements did not get in the way of the Committee's mission. The Committee was also helped by its record of avoiding leaks.[26] In contrast to the Church Committee, the parallel House committee floundered at the outset and floundered at the end on issues of secrecy.[27]

Having Empathy for but Maintaining Distance from the Agencies Being Overseen

The Church Committee started with the premise that "properly controlled and lawful intelligence is vital to the nation's interest." It is used, for example, to "monitor potential military threats . . . to verify compliance with international agreements . . . and to combat espionage and international terrorism."[28] In addition, fairness also required understanding for the difficult problems of the men and women who worked for the intelligence agencies. The government gave them assignments that were in many ways impossible to fulfill. They were expected to predict or prevent every possible crisis, respond immediately with information on any question, act to meet all threats, and anticipate and respond to the demands of presidents. Under that kind of pressure, is it any wonder that some cut corners? An additional point of perspective is that the illegal, improper, indecent, and silly conduct of some should not and does not indict whole agencies like the FBI and CIA that in the past and today perform vital work for this country.

Nonetheless, while understanding and respect are both necessary and appropriate, distance is also required. Many oversight bodies stumble by becoming too close to or advocates for the agencies they are meant to oversee. Moreover, agencies may try to divert overseers from their job—as FBI headquarters did in their first meeting with the Committee's chief counsel by showing pictures of severed heads on a city street. Certainly, the world of intelligence deals with many dangers. But the issue for oversight remained whether the agencies had

been "governed and controlled in accord with the fundamental principles of our constitutional system of government," and whether they had done things that were "illegal, improper and unethical."[29]

A SUMMARY OF THE FACTS CONCERNING THE RIGHTS OF AMERICANS

The Church Committee concluded that too much was collected from too many for too long. What was collected was distributed far too broadly. Excessively intrusive (and often knowingly illegal) techniques were used to gather intelligence. Covert action—secret punishment—was used to harass, disrupt, discredit, and destroy law-abiding citizens and domestic groups. Vague language in statutes and instructions by high officials facilitated abuses. There was waste and inefficiency. There was political abuse of intelligence information by presidents and by the intelligence agencies, who sometimes distorted the facts on important national issues like civil rights and the Vietnam War. Finally, the law and the U.S. Constitution were repeatedly violated and often simply ignored. Extensive documentation of all these findings is in the Committee's reports and hearings. Here are just a few illustrative examples.

Too Much Was Collected from Too Many for Too Long

The NAACP was infiltrated by government informers for twenty-six years, even though it was clear from the outset that its purposes were entirely lawful.[30] The FBI also conducted a broad-scale investigation of the Women's Liberation Movement. Meetings of women all over the country were infiltrated. Voluminous reports were filed on their beliefs. And once this spying started, it just kept going in blind disregard of its total irrelevance to any lawful government interest. Thus, one lengthy report concluded that the purpose of the infiltrated women's gathering had been to "free women from the humdrum existence of being only a wife and mother." Based on that, was the investigation stopped? No, the recommendation was to keep on investigating.[31] The CIA's Operation Chaos also investigated the Women's Liberation Movement, even though the CIA was barred by the act that created it from "internal security functions."[32]

The Socialist Workers Party was infiltrated by government informers for forty years—even though bureau officials conceded it had not committed any crimes and that its rhetoric fell far short of incitement to violence. When the man in charge of that investigation was asked what sort of information was passed back to the FBI, he replied that it included their political positions on the "Vietnam War," on "food prices," on "racial matters," on "U.S. involvement in Angola," and on any of the Party's efforts to support a non-Party candidate for office.[33] That's a pretty wide net.

The numbers of people affected are further proof of how pervasive the government's surveillance network became.

- The FBI opened over 500,000 domestic intelligence files, each of which typically contained names of several individuals.[34]
- The NSA obtained copies of millions of international cables. Indeed, from 1947 until 1975 it obtained copies of every single cable sent by individuals or businesses from this country to overseas locations.[35]
- The Army investigated some 100,000 Americans for political reasons between the mid-1960s and 1971. These included such vitally important matters as a Catholic priests' conference on birth control in Colorado, and a Halloween party of Washington schoolchildren which was investigated because the Army suspected a local "dissident" would be present.[36]
- The CIA's illegal mail opening program produced a computerized index of nearly 1.5 million names.[37]

Against these huge numbers, the FBI's secret list of 26,000 citizens to be rounded up in the event of a national emergency pales by comparison. But how broad the Bureau's version of the threat was perceived to be is illustrated by two names on that list—Dr. King and Norman Mailer. Mailer was on a list of persons who would have to be locked up because of "subversive associations and ideology." This list included: professors, teachers, and educators; labor union organizers and leaders; writers, lecturers, newsmen and others in the mass media field, scientists, doctors and lawyers. King was also characterized as subversive.[38]

Surveillance Techniques

In addition to infiltrating many lawful domestic groups like the NAACP, the Socialist Workers Party, and the Women's Liberation Movement, intelligence agencies used techniques like break-ins, mail opening, wiretaps, and bugs.[39] Break-ins and mail opening were both conceded as illegal. Nonetheless, they were justified internally by the vague words subversion and national security.[40] In each case, the illegal program followed the pattern of expanding enormously as time went on. Thus, for example, the CIA's watch list for opening letters started with fewer than twenty names, but by the late 1960s had grown to approximately 600, including many citizens and organizations engaged in purely lawful and constitutionally protected protest against government policies. Among the domestic organizations on the list were Clergy and Laymen Concerned About Vietnam, *Ramparts* magazine, the Student Non-Violent Coordinating Committee, and the American Friends Service Committee. But it was not just people on a watch list who had their mail opened. Many others had their letters unsealed and read, including Senator Frank Church and author John Steinbeck. During the

1968 presidential campaign, the CIA opened a letter passing between a speech writer and Richard Nixon.[41]

Warrantless wiretaps and bugs can be seen as a more complicated story. But the essence is simple. Every time Congress or the Supreme Court restrained use of these techniques, the executive branch secretly evaded the restrictions. For example, after the Supreme Court applied to federal agents a congressional limit on warrantless wiretaps, Attorney General Robert Jackson ordered the FBI to stop such wiretaps. But President Roosevelt overruled his attorney general, saying (in a "confidential memorandum") that he was sure the Court did not mean to require warrants for "persons suspected of subversive activities against the United States." As with his earlier order to FBI Director Hoover, however, Roosevelt did not explain what he thought "subversive" meant or why warrants could not be sought. A decade later, the Supreme Court reaffirmed that evidence obtained from a warrantless bug that had been placed in a house through a break-in could not be used in a criminal prosecution. The Court was particularly offended by the microphone being planted in a bedroom. But just after this ruling, Herbert Brownell, attorney general in the Eisenhower administration, sent a secret memo to Hoover authorizing the continued "unrestricted use" of bugs whenever the Bureau concluded it was in the "national interest." Brownell said the FBI did not even have to inform the attorney general. This secret order, using fuzzy phrases like "national interest," again manifested a clear disregard for the law and opened the door for many abuses, such as the bugs of Dr. King's hotel rooms.[42]

Congress, supposedly responsible for overseeing the FBI, failed to uncover any of this for decades. But as the Church Committee concluded after its exhaustive look at all important activities of the intelligence agencies over more than three decades: "The imprecision and manipulation of labels, such as 'national security,' 'domestic security,' 'subversive activities' and 'foreign intelligence' have led to unjustified use" of methods like wiretaps and bugs, and excessive surveillance of Americans.[43]

Domestic Covert Action

Echoing the COINTELPRO effort to cause "violent reprisals" against the leader of the Chicago Black Panthers, the San Diego FBI office boasted about how our most respected law-enforcement agency was fomenting violence: "Shootings, beatings, and a high degree of unrest continues to prevail in the ghetto area of southeast San Diego. Although no specific counter-intelligence action can be *credited* with contributing to this overall situation, it is felt that a substantial amount of the unrest is directly attributable to [COINTELPRO]."[44]

There was much more to the FBI's campaign to destroy Martin Luther King than a note intended to provoke a suicide. After King's "I Have a Dream" speech, the FBI's Domestic Intelligence Division concluded that this "demagogic speech" established Dr. King as the nation's "most dangerous Negro leader." The FBI decided to "take him off his pedestal." It decided to secretly select and

promote its own candidate to "assume the role of the leadership of the Negro people." Later, Bureau headquarters explained to the field that King must be destroyed, because he was seen as a potential messiah who could "unify and electrify" the "black nationalist movement." King was then described as a threat because he might "abandon his supposed 'obedience' to white liberal doctrines (non-violence)."[45] In short, a nonviolent man was to be secretly attacked and destroyed as insurance against his abandoning nonviolence.

The effort to destroy King was part of COINTELPRO, which meant illegal investigations and secret punishment, administered not by a court but by the government's chief law enforcement agency. Its aim was not a public arrest or a judicial trial, but a secret program to "harass and disrupt" dissidents and others deemed to be unacceptable. COINTELPRO's tactics were designed, for example, to break up marriages of civil rights workers, get teachers fired, destroy reputations of lawyers, sabotage political campaigns, encourage violent retribution by falsely and anonymously labeling intended victims as government informers, and stop citizens from speaking, teaching, writing, or publishing.[46]

COINTELPRO "resulted in part from frustration with Supreme Court rulings limiting the government's power to proceed overtly against dissident groups."[47] The government had the right and duty to prosecute lawless acts done, for example, by the Black Panthers or the Ku Klux Klan. But it had no right to secretly usurp the functions of judge and jury by covertly taking the law into its own hands. It had no right to try to foment deadly gang warfare against the Black Panthers. And it had no right to send dirty anonymous letters to the wife of a Klan member seeking to break up her marriage.[48]

The targets of COINTELPRO were not limited to the famous like Dr. King or those on the fringes of law abiding society like members of the Klan or the Black Panthers. Thus, among hundreds of examples:

- The Unitarian Society of Cleveland was targeted because its minister and some members had circulated a petition calling for the abolition of the House Un-American Activities Committee.[49]
- "Disinformation" concerning housing was sent to demonstrators coming to Chicago for the 1968 Democratic National Convention to cause them "long and useless journeys."[50]
- Nonviolent citizens who were against the Vietnam War were targeted because they gave "aid and comfort" to violent demonstrators by lending respectability to their cause.[51]

Political Abuse

All administrations from Franklin Roosevelt to Richard Nixon asked for and got political information from the FBI.[52] But there was a marked increase during the Johnson and Nixon administrations. Much of the information obtained was

derogatory and personal. Most of the information reflected the FBI's having collected and filed too much from too many for too long.

- Examples of information asked for by the Johnson White House: during the closing days of the 1964 campaign, on all persons employed in the Senate Office of Senator Barry Goldwater (R-AZ); in the 1968 campaign, on vice presidential candidate Spiro Agnew's long-distance telephone calls; on seven senators who criticized bombing of North Vietnam; on all people who signed letters to Senator Wayne Morse (D-OR), supporting his criticism of the Vietnam War; on many mainstream journalists, including NBC anchor David Brinkley and *Life Magazine*'s Washington Bureau chief; and on authors of books critical of the Warren Commission report on the assassination of President Kennedy. For the Democratic Convention in Atlantic City in 1964, President Johnson directed the assignment of an FBI "special squad." Perhaps the original purpose was to guard against civil disorders. But as so often was the case, what started modestly grew beyond the pale. For example, the FBI sent many memos to the White House from the convention reporting on the political plans of the Mississippi Freedom Democratic Party and of Dr. King.[53]
- Examples of information asked for by the Nixon White House: on CBS reporter Daniel Schorr; on the Chairman of Americans for Democratic Action; on Ralph Abernathy (Dr. King's successor as head of the Southern Christian Leadership Conference) for the purpose of "destroying his credibility." The administration also received the fruits of warrantless wiretaps, lasting from 1969 to 1971 in a leak investigation of three newsmen and fourteen executive branch employees. Again this shows a widening of surveillance far beyond the purported reason for seeking the taps. The information reported was not focused on leaks but included: a report on a plan of Senator Edward Kennedy (D-MA) to give a speech on Vietnam; the planned timing of Senator J. William Fulbright's (D-AK) hearings on Vietnam; Senator Mondale's "dilemma" about a trade bill; and, what former President Johnson had said about the candidacy of Senator Edmund Muskie (D-ME) for the Democratic presidential nomination. The wiretaps continued on two targets after they left government to work on Muskie's campaign. (Revealingly, the memos began to be sent to H. R. Haldeman, the President's political advisor, rather than Henry Kissinger, who had first demanded the warrantless wiretaps for "national security reasons.")[54]

The FBI also used intelligence information to influence social policy and political action on the most important national issues, including civil rights and Vietnam.

In 1956, the FBI sent memos to the White House about the NAACP (which it had secretly infiltrated). In general, it suggested that communist or communist-front organizations were causing "a marked deterioration in relationships between the races." Director Hoover briefed the Eisenhower Cabinet on alleged

communist influence in the civil rights movement. According to one historical account, this briefing "reinforced the President's passivity" on civil rights legislation.[55]

In 1963, the Bureau's Domestic Intelligence Division submitted to Hoover a memo detailing the Communist Party's "efforts" to exploit black Americans. It concluded the efforts were an "obvious failure." Hoover was not pleased. He made clear "we had to change our ways or we would all be out on the street." A new memo was sent: "The Director is Correct." Dr. King was the "most dangerous Negro" from the "standpoint of communism . . . and national security." It was "unrealistic" to limit ourselves to "conclusive proofs." Communist Party influence over Negroes "one day *could* become decisive." When the Hoover subsequently testified to Congress, he said communist influence *was* "vitally important."[56]

On Vietnam, President Johnson told Hoover he had "no doubt" communists were behind the demonstrations against the Vietnam War. Hoover agreed. Back at the FBI, Hoover told his associates that he knew the Bureau might not be able to "technically state" what the President wanted. But he wanted and got a "good, strong memorandum" that made communist "efforts" sound like communist success.[57]

The Law: Breaking It, Ignoring It, and Fuzzy Words Replacing It

The Church Committee uncovered lots of illegal, improper, and immoral conduct, which can only be touched on here.[58] What did the actors think about what they were doing? Did the vague and fuzzy secret instructions and the pressure they got from presidents and other high officials open the door to misconduct?

Many never gave a thought to the law or the Constitution. As the man who headed the FBI's Domestic Intelligence Division for ten years testified: "Never once did I hear anybody, including myself, raise the question: 'Is this course of action which we have agreed upon lawful, is it legal, is it ethical or moral.' We never gave any thought to this line of reasoning, because we were just naturally pragmatic."[59] Similarly, the White House author of the Huston Plan (see Volume 4, Appendix B), where the heads of the major intelligence agencies proposed to President Nixon knowingly illegal mail opening and break-ins (not saying the proposed actions were already actually being done), testified that nobody at the meetings ever objected to undertaking illegal acts—indeed legality or constitutionality was never discussed.[60]

The first reaction of the National Security Agency's general counsel to learning that the Committee had found out that for decades the NSA had illegally obtained every single cable sent out of the United States by Americans was that the Constitution and the law did not apply to the NSA because it worked on "foreign" intelligence. Similarly, when asked if he was concerned about the legality of the NSA's warrantless interceptions of electronic communications, the agency's deputy director replied: "That particular aspect didn't enter into the discussions."[61]

And when the former head of the Bureau's Racial Intelligence Section was asked whether during COINTELPRO's history anybody at the FBI discussed its constitutionality or legality, he answered, "no, we never gave it a thought."[62]

Of course, there were many others who did think about legality and who clearly knew their actions were illegal. For example, at least four internal memoranda recognized that the CIA's mail opening program had "no legal basis," that "federal statutes preclude the concoction of any legal excuse," and that exposure could "give rise to grave charges of criminal misuse of the mails by government agencies."[63] Similarly, despite receiving advice from the Federal Communications Commission that its monitoring of the radio communications of amateur radio operators was illegal, the Army Security Agency plowed ahead with the monitoring.[64]

The CIA's experiments with the effect of drugs such as LSD started with volunteers but moved to unsuspecting victims—or in the Agency's sterile jargon, "unwitting subjects"—at "all social levels, high and low, native American and foreign." Recognizing that drugging unknowing subjects was illegal and potentially dangerous, Richard Helms, who later became Director of Central Intelligence, successfully sought approval: "While I share your uneasiness and distrust for any program which tends to intrude on an individual's private and legal prerogatives, I believe it is necessary that the agency maintain a central role in this activity." One of the subjects was Dr. Frank Olson, a scientist working with the U.S. Army Biological Center. At a conference of CIA and Army scientists, he was given a dose of Cointreau laced with LSD. He later died.

Knowledge of the CIA's illegal and unethical drug experiments was kept secret for decades, because, as the CIA's Inspector General wrote: "Precautions must be taken not only to protect operations from exposure to enemy forces, but also to conceal these activities from the American public in general. The knowledge that the Agency is engaging in unethical and illicit activities would have serious repercussions in political and diplomatic circles and would be detrimental to the accomplishment of its mission." After Olson's death had dramatized the dangers, the Agency continued to experiment with unwitting subjects for ten years. Those involved in Olson's doping were given a letter from CIA Director Allen Dulles that criticized them for not giving "proper consideration to the rights of the individual to whom it was being administered." But Helms was instructed to inform them that the letter was "not [a] reprimand," and that no personnel file notation was made.[65]

OBSERVATIONS REGARDING OVERSIGHT OF AMERICA'S FOREIGN INTELLIGENCE AGENCIES

Given space limitations (and the fact that after completion of the Assassinations Report, I did not focus on foreign intelligence), I make only a few points about foreign intelligence here. To begin with, before the Church Committee,

congressional oversight of the CIA and other foreign intelligence agencies was an embarrassment. The Senate and House intelligence oversight subcommittees lacked written records, and often they asked no questions; never did they ask tough questions. As Clark Clifford reflected later, "Congress chose not to be involved and preferred to be uniformed." A longtime CIA general counsel concluded that the lack of congressional oversight ultimately caused *problems* for the Agency because "we became a little cocky about what we could do."[66]

William Colby, CIA director during most of the Church Committee investigation, reached a similar conclusion. The congressional investigations were "necessary" and "effective." "This year's excitement," he wrote in a February 1976 *New York Times* op ed piece, "has made clear that the rule of law applies to all parts of the American Government, including intelligence . . . this will strengthen American intelligence."[67] In its *Final Report*, Book I, the Church Committee provided extensive analysis of the strengths and weaknesses of America's foreign intelligence agencies, calling, for example, for more attention to be given to human intelligence—that is, regular spying.

VALUES SUSTAIN INVESTIGATIONS

Having obtained and disclosed the facts, the Committee had to answer two big questions that depend on values.

- Should the United States, faced with a powerful, often unscrupulous, and sometimes vicious enemy adopt the enemy's tactics?
- Should Congress—and the American public—be trusted with the truth?

The Committee first publicly addressed these questions in its report on assassinations.

On November 20, 1975, the Senate convened in executive session to discuss the Committee's *Interim Report* on assassination plots. All eleven Committee members had signed the report. However, President Ford and CIA Director Colby opposed its public release. At this executive session, the first crack in the Committee's unity began to appear. Senator Barry Goldwater said he had signed the report only as "an act of gratitude for the hard work done by the Committee and the staff"; public release of the report would be a "spectacle of public self-flagellation" that would hurt our reputation abroad. On the Senate floor, Senator Tower who, along with Senators Church and Gary Hart (D-CO), had been the Committee members on a subcommittee that worked for weeks on the report before it was presented to the full Committee, said he was "distressed and sorry," but he wanted "to publicly disassociate [himself] from public release of the report" because a number of senators had decided they did not want to vote on the issue of public release.[68] After several hours of discussion, but without any vote against (or for) release, the report was issued when the Senate adjourned shortly after 1 P.M.[69]

Beyond the fascinating stories about plot details (see, e.g., Volume 3, Appendix F) and beyond the question of presidential authorizations lay key principles—key then and key today. Should the United States, when faced by unscrupulous enemies, adopt their tactics? Should the American people be allowed to know what their government had been doing? Would doing so harm our reputation in the rest of the world?

The Committee's work as a whole stands as answers to these questions. Those answers were first expressed publicly in the assassinations report whose last words, in an epilogue, were:

> The Committee does not believe that the acts which it has examined represent the real American character. They do not reflect the ideals which have given the people of this country and of the world hope for a better, fuller, fairer life. The United States must not adopt the tactics of the enemy. Means are as important as ends. Crisis makes it tempting to ignore the wise restraints that make men free. But each time we do so, each time the means we use are wrong, our inner strength, the strength which makes us free, is lessened. Despite our distaste for what we have seen, we have great faith in this country. The story is sad, but this country has the strength to hear the story and to learn from it. We must remain a people who confront our mistakes and resolve not to repeat them. If we do not, we will decline; but, if we do, our future will be worthy of the best of our past.[70]

There have been, of course, those who say the tactics of the enemy *should* be adopted. They claim necessity. Thus, for example, in 1954 the secret report of a special committee, formed to advise President Eisenhower on covert activities, said the United States may have to adopt tactics "more ruthless than those employed by the enemy." "Hitherto acceptable norms of human conduct do not apply." "Long standing American concepts of American fair play must be reconsidered."[71]

The Church Committee noted that "it may well be ourselves that we injure most if we adopt tactics more ruthless than the enemy's."[72] And the committee's *Foreign and Military Intelligence Report* concluded that those planning covert actions "rarely noted" the possible harm the actions could cause to "this nation's ability to exercise moral and political leadership throughout the world."[73]

Throughout, the Church Committee's view was that the United States must not adopt the tactics of the enemy. On this, the Ccommittee members never wavered, never split.

On the second big question—whether the American public could be trusted with the truth—the Committee also remained united that the embarrassing and unseemly revelations in the report on *Intelligence Activities and the Rights of Americans* should be made public. Indeed, Senators Robert Morgan (D-NC) and Howard Baker (R-TN) in their additional statements commented (in a bipartisan way) on the favorable impact of making the *Rights of Americans* Report public.

- Morgan: "Releasing this report is a great testament to the freedom for which America stands." He added, "It is my sincere hope that the Report . . . will rekindle in each of us the belief that perhaps our greatest strength lies in our ability to deal frankly, openly and honestly with the problems of our government."[74]
- Baker: While disagreeing (articulately as always) with a number of the Committee's recommendations for reform, Baker opined that the abuses being "fully aired to the American people" would have a "cathartic effect" on the FBI and CIA. (He supported this conclusion by quoting the article by former CIA Director Colby that said "this year's excitement" will "strengthen American intelligence.") Baker added: "It is important to disclose to the American public all of the instances of wrongdoing we discovered."[75]

Earlier, Senator Charles M. Mathias (R-MD) provided eloquent and concise views on both the two big values questions:

- "Painful political problems are seldom solved by silence. As crude as the story unfolded here may seem, it can be the source of important lessons for the future." And, quoting James Madison, he said, "Knowledge will forever govern ignorance and a people who mean to be their own Governors must arm themselves with the power which knowledge gives," adding, the Committee "sought to stop the erosion of society's values caused by excessive secrecy and unchecked Executive power by making the factual record as accurate and clear as possible."
- "History shows that men and governments have come to recognize the compelling force of ethical principles. The torturer who was once an adjunct of the courts themselves is today an international outlaw. By recognizing the sacredness of human life, mankind has sought to shed such barbarisms, barbarisms that have usually led to further violence and often to the destruction of the leaders and nations who resorted to them."[76]

WRESTLING WITH RESPONSIBILITY

On the question whether presidents, attorneys general, and other high-level officials in the executive branch were responsible for the many acts of agency misconduct recounted in the Committee's reports, the Committee's thinking evolved toward a "yes" answer.

Early in the assassinations investigation, Senator Church speculated to the press that the CIA may have acted as a "rogue elephant on a rampage," conceiving and carrying out the plots without authorization from outside the agency.

In contrast, other senators, also speculating, opined that the CIA "took orders from the top."[77]

When the assassinations report was issued several months later, the Committee rejected both theories, demonstrating that there was support for either conclusion but saying the conflicting evidence made it impossible to be sure whether Presidents Eisenhower and Kennedy (both dead for many years) had authorized the plots during their administrations. (The Committee found that President Johnson had not.[78])

Five months later, when it issued its final reports covering the gamut of its investigation, the Committee was ready to fix responsibility at the top. In the *Final Report on Foreign and Military Intelligence* (*Book I*), the Committee concluded: "On occasion, intelligence agencies concealed their programs from those in higher authority; more frequently, it was the senior officials themselves who, though pressure for results created the climate within which the abuses occurred."[79]

The Final Report on Intelligence Activities and the Rights of Americans (*Book II*) reached the same ultimate conclusion with more details. Though intelligence agencies did, on occasion, fail to reveal their programs or acts to their superiors, "the most serious breaches of duty were those of senior officials who were responsible for controlling intelligence activities and generally failed to assure compliance with the law."[80] The Committee elaborated: fault at the top was shown by "demanding results" without paying attention to means, "failing to inquire further" after receiving indications that improper activities had been occurring, delegating broad authority using fuzzy phrases like "national security" or "subversion" and then failing to require adequate guidelines or procedural checks on what actually was done, and "exhibiting a reluctance to know about secret details of programs."[81]

The change in emphasis as the Committee's work progressed was the product of exposure to the whole record. Looking at specific agency acts individually sometimes did show the agencies acting on their own, or even misleading their superiors. But when the full record, over many years, was examined, ultimate responsibility was properly fixed with the presidents, attorneys general, and other high executive branch officials for the sorts of reasons already outlined. To the Committee's chief counsel looking backward thirty years later, it seems there were also at least three more reasons to fix that ultimate responsibility with higher authority. The power of the FBI was such that although it was wrong, it was not surprising that attorneys general exercised only weak oversight. But they knew that was what they were doing. The doctrine of plausible denial was originally designed to implement covert actions overseas in a way calculated to conceal American involvement if the actions were exposed. The doctrine was then extended to the internal decision-making processes of the government itself. As explained by Richard Bissell (the principal CIA architect of the assassination plots), the Director of the CIA (Allen Dulles, who was dead) was supposed to have informed the presidents of the plots (and other covert actions) by talking

"circumlocutiously."[82] The Committee described the doctrine of plausible deniability as "a delusion and at times a snare."[83]

One consequence of plausible denial was that witnesses before the Committee constantly confronted it with a bureaucratic shell game. High-level officials, generally outside the agencies, repeatedly disclaimed knowledge of improper or illegal activities—and suggested that agency personnel were concealing their own nefarious acts. Officials within the agencies consistently said they had the *tacit* approval of their superiors, and suggested the superiors were dissembling about their knowledge and approval. The Committee found both accusations to be true at times. But it found in all cases that the authorization and responsibility facts were confused. It seems likely that both bosses and operatives found that useful. It is certain that ambiguity as to authorization increases the risk of abuse.

However one cuts through the fog of plausible deniability to decide who was responsible for any given action, what is crystal clear is that the presidents, national security advisors, and other high executive branch officials knew about the plausible deniability system. Therefore, if—and this is a big if—they did not know about a particular action, they were nonetheless culpable because they had knowingly turned a blind eye to what was going on.

Finally, presidents and other high-level executive branch officials also knew that all intelligence activities, domestic and foreign, were smothered in layers of excess secrecy. They knew that Congress and the courts played no meaningful role. And they knew (or should have known) that the combination of excessive secrecy, the absence of checks and balances, and the use of fuzzy, vague authorizations were (as they remain today) a recipe for excess and abuse.

SOME GENERAL LESSONS

First, prolongation of crisis is particularly hard for constitutional democracies. There were more than thirty years between Franklin Roosevelt's reinstitution of an open-ended, secret (indeed concealed), and poorly controlled security regime and Nixon's fall. For all this time, America was at war, or in a Cold War. It felt beleaguered. To refer again to the language of the Church Committee report on assassinations, crisis "makes it tempting to ignore the wise restraints that make men free," and to use means that are wrong—means that lessen "our inner strength, the strength that makes us free," as well as undermining the reputation that helps make us strong.

Second, a perfect storm of institutional shortcomings stirred a brew of immoral or illegal acts that could not be squared with a "decent respect to the opinions of mankind." It was not evil that caused us to do what we ought not to have done. It was zeal, fostered by excessive secrecy; vague instructions and implicit nudges or winks joined to pressure for results without attention to means; and oversight that was either lacking altogether, empty, or knowingly chose to turn a blind eye.

Third, foolish secrecy fertilizes the soil from which abuse grows. Clearly, there is much about intelligence work that is properly kept secret. Examples such as the names of agents and technological details of collection methods are obvious. Nonetheless, unnecessary secrecy served to inhibit and often prevent any sober review of the basic programs and practices themselves. If a tactic cannot survive the light of day, it likely should not be born. A related point is that seldom, if ever, were the consequences of exposure weighed before a program was begun. Similarly, a foolish expectation of perpetual secrecy increased the likelihood that the harmful effect on America's reputation of adopting the tactics of the enemy would be ignored.

Fourth, secrecy was the handmaiden of blinded oversight—or sometimes intentionally blind oversight. Congress played no meaningful role. Congress is not perfect, but it can add wisdom and help avoid mistakes. Because of excessive secrecy, the good sense of the American public was also barred from any debate.

Fifth, whatever the explanation for the use of euphemisms or simple falsehoods to describe or justify dirty business, it seems certain that failure to call dirty business by its rightful name increases the chance of dirty business being done. Words about dirty business were often sterilized. For example, Bissell thought CIA directors should talk to presidents about killing using euphemisms or circumlocuitous language. (Even years later, during the Committee's investigation, those who had worked on killings could not bring themselves to use simple, honest, direct words to describe what they had done. Instead, just as in the contemporaneous documents, they used phrases such as "dispose of," or "get rid of," or "eliminate," or some such euphemistic circumlocution.) Similarly, when Richard Helms recommended that the CIA continue to experiment by giving drugs to unwitting subjects, he used sanitized, bleached, and lifeless words—"uneasiness," "distaste," "tends to intrude"—about stark realities of death and lawlessness. Finally, when Bureau officials used Orwellian language to describe Martin Luther King Jr. as the leader of a black nationalist "hate" group, perhaps deep down they hoped to feel better about the dirty business they set out to do.

Sixth, every intelligence program we looked at started with investigating, harassing, or attempting to destroy targets who were on the fringes of law-abiding society and then moved progressively further toward mainstream dissidents and finally began to cover ordinary citizens. Thus, as shown, the CIA's knowingly illegal mail opening program was initially advocated as a way to catch foreign spies and ended up checking up on organizations like the American Friends Service Committee. COINTELPRO started by harassing the U.S. Communist Party and ended by harassing hippies. The NSA started by decoding encrypted telegrams from foreign embassies and widened its net to include anti–Vietnam War and civil rights protestors.

In criticizing his own earlier efforts, Tom Charles Huston (White House coordinator of the Huston Plan in which the CIA, the NSA, and other intelligence agencies sought official sanction for lawlessness for things they had long been doing and which they continued to do after President Nixon rescinded his written

approval) put well the tendency for the net to widen. There is, he testified to the Committee, the risk that governmental surveillance would: "Move from the kid with a bomb to the kid with a picket sign, and from the kid with the picket sign to the kid with the bumper sticker of the opposing candidate. And you just keep going down the line."[84]

Seventh, those who conclude that reform is needed need to make their case based on facts exposing wrongdoing. Nonetheless, a "Senate Committee is not a prosecutor, a grand jury or a court." It is far better suited to determine how things went wrong and what can be done to prevent their going wrong again, than to resolve disputed questions of individual "guilt" or "innocence."[85]

Congressional committees or citizen commissions that fail to recognize this distinction make splashes, but not waves. As the Church Committee said, they provoke a national debate on "who did it," not on "how did it happen and what can be done to keep it from happening again?"[86]

NOTES

1. The Church Committee reports cited most extensively are: *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate: Foreign and Military Intelligence* (Washington, DC: Government Printing Office, 1976), hereafter Bk. I; Book II: *Intelligence Activities and the Rights of Americans* (Washington, DC: Government Printing Office, 1976), hereafter Bk. II; Book III: *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans* (Washington, DC: Government Printing Office, 1976), hereafter Bk. III; *Interim Report: Alleged Assassination Plots Involving Foreign Leaders* (Washington, DC: Government Printing Office, 1975), hereafter *Assassinations*. The seven volumes of Church Committee hearings are *Hearings Before the Select Committee to Study Government Operations with Respect to Intelligence Activities of the United States Senate, Volume 1: Unauthorized Storage of Toxic Agents; Volume 2: Huston Plan*; *Volume 3: Internal Revenue Service; Volume 4: Mail Opening; Volume 5: The National Security Agency and Fourth Amendment Rights; Volume 6: Federal Bureau of Investigation*; and *Volume 7: Covert Action* (Washington. DC: Government Printing Office, 1976). A full text archive of all reports and hearings of the Church Committee is available online at http://www.aarclibrary.org/publib/church/reports/contents.htm. Books on the Church Committee include Loch K. Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (Lexington: University Press of Kentucky, 1985); Frank J. Smist, *Congress Oversees the United States Intelligence Community*, *1947–1994* (Knoxville: University of Tennessee Press, 1994), esp. chap, 2; LeRoy Ashby and Rod Gramer, *Fighting the Odds: The Life of Senator Frank Church* (Pullman: Washington State University Press, 1994), esp. chap. 16, pp. 453–92.

2. See Bk. II, p. viii.

3. Senate Resolution 21, January 27, 1975. The resolution is also an appendix to Johnson, *A Season of Inquiry*.

4. For the FBI's treatment of King generally, see Bk. II, pp. 11–12, 219–23, and Bk. III, "Dr. Martin Luther King, Jr., Case Study," pp. 79–184. For "hate group," see Bk. III,

pp. 179–80. For effort designed to get King to commit suicide, see Bk. II, pp. 11 and 220–21, and Bk. III, pp. 158–61.

5. For Castro plots, see *Assassinations*, pp. 17–180, 255, 257, 263–70, 270, 274–77.

6. See Johnson, *Season of Inquiry*, p. 9, for reference to various articles, including Hersh's.

7. For a summary of these disputes and their resolution, see Johnson, *Season of Inquiry*, pp. 27–44, 45–48.

8. This incident is described in *Assassinations*, pp. 129–30.

9. For "brought home," see Bk. II, p. 212n.7.

10. Johnson, *Season of Inquiry*, pp. 23–44, 86, 125–29, 273.

11. Smist, *Congress Oversees*, pp. 19–24.

12. Ibid., chap. 2, pp. 25–82.

13. For the Church Committee's history of the FBI, see Bk. II, "The Growth of Domestic Intelligence," pp. 21–136, and Bk. III, "The Development of FBI Domestic Intelligence Investigations," pp. 373–538. The FBI's antecedents and its early history are in Bk. II, pp. 23–28, and Bk. III, pp. 378–400. For the Committee's history of the CIA, see Bk. I, pp. 97–125.

14. For Stone's views on the Bureau and his policy announcement, see Bk. II, pp. 23–24; Bk. III, pp. 388–95.

15. See Bk. III, pp. 384, 391.

16. The Roosevelt memos and Hoover's records of conversations with Roosevelt are set out in Bk. III, pp. 391–406 and summarized in Bk. II, pp. 24–27.

17. For the League for Fair Play, see Bk. II, p. 32, and Bk. III, p. 415. For the NAACP, see Bk. III, p. 416. For Lindbergh, see Bk. II, p. 33.

18. For "periodic public scrutiny," see *Hearings Before the Selection Committee to Study Government Operations with Respect to Intelligence Activities of the United States Senate, Volume 6: Federal Bureau of Investigation* (Washington: Government Printing Office, 1975), p. 1. For "establishing a complete and open record," see ibid., p. 3.

19. Ibid., pp. 4–40.

20. Ibid., p. 41.

21. Johnson, *Season of Inquiry*, p. 129.

22. For "ugly little acronym," see Frederick A. O. Schwarz Jr., "Intelligence Activities and the Rights of Americans,"*The Record of the Association of the Bar of the City of New York* 32, no. 1/2 (January/February 1977), pp. 43, 46. For COINTELPRO generally, see Bk. II, pp. 10–12, 65–94, 211–23. See also Bk. III, "COINTELPRO: The FBI's Covert Action Programs Against American Citizens," pp. 1–79.

23. Bk. II, pp. 271–72n.20.

24. See Johnson, *Season of Inquiry*, p. 43.

25. See Staff Report on *Covert Action in Chile, 1963–75*, preface.

26. There were only two leaks stemming from the Church Committee. One included information about Kennedy's romantic relationship to the person whom the Committee's report described as a mutual "friend" of the President and the mafia boss hired to kill Castro. The other involved a staff member who was overheard in a restaurant discussing a position that had been taken by a Senator (not on the Committee) in connection with oversight. (The staffer was fired.) Neither leak affected national security. See Smist, *Congress Oversees*, 38, 48–49.

27. See Smist, *Congress Oversees*, chap. 4, pp. 134–213, particularly pp. 136–37, 143, 156–57, 169–71, 175–76, 183–87, 211–13.

28. Bk. II, p. v.

29. Bk. II; Senate Resolution 21.

30. For general discussion of too much information being collected, see Bk. II, pp. 6–10, 165–82. For NAACP, see Bk. II, pp. 8, 179–80.

31. Bk. II, p. 7.

32. Ibid., p.102.

33. Ibid., p.180.

34. Ibid., p. 6.

35. For the numbers, see Bk. II, pp. 6, 12; Bk. III, p. 740 ("the largest governmental interception program affecting Americans"). For the NSA generally, see Bk. II, pp. 6, 12, 104, 210–12; Bk. III, "National Security Agency Surveillance Affecting Americans," pp. 733–83.

36. For the numbers, see Bk. II, p. 6. For the birth control conference and Halloween party, see Bk. II, p. 8. For Army investigations generally, see Bk. II, pp. 77, 167, and Bk. III, "Improper Surveillance of Private Citizens by the Military," pp. 785–834.

37. See Bk. II, p. 6. For the CIA (and FBI) illegal mail opening programs, see Bk. III, "Domestic CIA and FBI Mail Opening," pp. 559–677.

38. For general discussion of the Bureau's detention lists, see Bk. II, pp. 54–56, and Bk. III, pp. 436–47, 510–16, 542–48. For the categories of detention and "subversive associations," see Bk. II, p. 55. For Mailer's inclusion on the list, see Bk. II, p. 56. For King's inclusion, see Bk. III, p. 87.

39. For break-ins generally, see Bk. II, pp. 61–62, 190–92, 204–5. See also Bk. III, "Warrantless Surreptitious Entries: FBI 'Black Bag' Break-Ins and Microphone Installations," pp. 353–71. For mail openings generally, see Bk. II, pp. 58–59, 190–92, 203. See also Bk. III, "Domestic CIA and FBI Mail Opening Programs,"pp. 559–677.

40. For illegal and combating subversion, see Bk. III, p. 358; for national security, see Bk. II, for example, pp. 141, 144, 145.

41. For growth in the CIA's watch list and the people and organizations covered, see Bk. II, pp. 208–9 and Bk. III, 573–74. For the letter to Nixon, see Bk. II, p. 8. For nearly 1.5 million names in a CIA database derived from mail-opening, see Bk. II, p. 6.

42. See Bk. III, pp. 278–79. Jackson reversed the Justice Department's policy concerning wiretapping in Order No. 3343, issued March 15, 1940, prohibiting all FBI wiretapping. Bk. III, p. 279, quoting memorandum from Roosevelt to Jackson, May 21, 1940; Bk. II, p. 190, quoting memorandum from Brownell to Hoover, May 20, 1954.

43. Bk. II, 205. See also Justice Robert H. Jackson's opinion in *Youngstown Sheet and Tube* referring to the "loose and irresponsible" use of "adjectives . . . without fixed or ascertainable meanings" like "inherent" or "war" powers. *Youngstown Sheet and Tube v. Sawyer*, 343 U.S. 579, 646–47 (1952).

44. Bk. II, p. 218 (emphasis added).

45. For "most dangerous and effective Negro leader," see Bk. II, p. 11, and Bk. III, pp. 107–9. For "take him off his pedestal" and "assume the role of the leadership," see Bk. II, p. 11, and Bk. III, pp. 136–37. For "hate group," see Bk. III, pp. 179–80. For "messiah," see Bk. II, pp. 11–12, and Bk. III, p. 180.

46. For examples of COINTELPRO methods, see Bk. II, pp. 216–19. See also Bk. III, pp. 7–8. For "embarrass the Bureau," see Bk. II, p. 156, quoting the FBI Manual.

47. See Bk. II, p. 211, and Bk. III, pp. 10–11. For the Smith Act, see 18 U.S.C. §2385 (which remains on the books); *Yates v. United States*, 354 U.S. 298 (1957); *Watkins v. United States*, 354 U.S. 178 (1957).

48. See Bk. II, pp. 216–17; Bk. III, COINTELPRO chapter, pp. 51–52.

49. Bk. II, p. 214n.14.

50. Ibid., p. 216n.34.

51. Ibid., p. 213. See also Bk. II, p. 214n.19.

52. For political uses generally, see Bk. II, pp. 225–52.

53. Bk. II, pp. 228–31, 235–36.

54. Ibid., pp. 230–31, 23–36.

55. See Bk. II, pp. 232–33. For "marked deterioration," see Bk. II, p. 233n.40. For Hoover's subsequent briefing, see Bk. II, pp. 250–51n.151a. For the historical account, see J. W. Anderson, *Eisenhower, Brownell, and the Congress: The Tangled Origins of the Civil Rights Bill of 1956–57* (Tuscaloosa: University of Alabama Press, 1964), p. 34.

56. Bk. II, p. 250, emphasis added.

57. Ibid., 251.

58. The Church Committee's first finding in *Intelligence Activities and the Rights of Americans* covered "Violating and Ignoring the Law," Bk. II, pp. 137–63.

59. Bk. II, pp. 14 and 141.

60. Ibid., 141.

61. Author's recollection of conversation with NSA general counsel. Testimony of NSA Deputy Director Benson Buffham, *Hearings Vol. 5: The National Security Agency and Fourth Amendment Rights*, p. 45.

62. Bk. II, p. 140.

63. Ibid., pp. 142–48.

64. Ibid., p. 144; and see generally Bk. III, "Improper Surveillance of Private Citizens by the Military," pp. 785–834.

65. For CIA drug experiments generally, see Bk. I, "CIA Drug Testing Programs," pp. 392–411. For "unwitting subjects," p. 391; Helms memo, p. 394; Olson story, pp. 394–99; I.G. memo, p. 394; continuation, p. 403; Dulles letter, pp. 398–99.

66. The Clifford and CIA general counsel quotes are in Smist, *Congress Oversees*, pp. 5 and 9.

67. William Colby, "After Investigating U.S. Intelligence," *New York Times*, (February 26, 1976), p. A30.

68. Johnson, *Season of Inquiry*, pp. 130–37.

69. Ibid.

70. *Assassinations*, epilogue, p. 285.

71. See James Doolittle, et al., *The Report on the Covert Activities of the Central Intelligence Agency*, September 30, 1954, quoted in Bk. I, p. 50, and *Assassinations*, p. 259n.1.

72. *Assassinations*, p. 259.

73. Bk. I, p. 156.

74. Bk. II, pp. 363–65.

75. Ibid., pp. 373–75.

76. *Assassinations*, pp. 345–46.

77. Johnson, *Season of Inquiry*, p. 57.

78. For authorization evidence and conclusions as seen in *Assassinations*, see pp. 6–7, 51–70 (Lumumba), 91–180 (Castro).

79. Bk. I, p. 137.

80. Bk. II, p. 137.

81. Ibid., pp. 139, 265.

82. *Assassinations*, pp. 111, 118.

83. For plausible deniability generally, see *Assassinations*, pp. 11–12, 277–78.

84. Bk. II, p. 4.

85. Ibid., viii.

86. Ibid. See also Aziz Huq and Frederick A. O. Schwarz Jr., *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (New York: New Press, 2007).

3

A CONVERSATION WITH FORMER DCI WILLIAM E. COLBY, SPYMASTER DURING THE "YEAR OF THE INTELLIGENCE WARS"

LOCH K. JOHNSON

AS EXAMINED IN THE PRECEDING CHAPTER, the Church Committee carried out a sweeping inquiry in 1975 into charges that the Central Intelligence Agency (CIA) had violated its charter by spying on citizens within the United States. This year is remembered by historians as the most extensive probe into the CIA since its founding in 1947. Many intelligence professionals inside the Agency recall the investigation as a period of great trauma—the Year of the Intelligence Wars between the CIA and Congress.[1] At the helm of U.S. intelligence at the time was William Egan Colby, the Director of Central Intelligence (DCI). In that capacity, he was the titular leader of the entire intelligence community and directly in charge of the CIA, where the office of the DCI was located at the time (and until 2005) on the Seventh Floor of the Agency's headquarters building in Langley, VA, adjacent to McLean.

As DCI, Colby conceded to *New York Times* reporter Seymour M. Hersh that a laundry list of wrongdoing by CIA officers, dubbed the "family jewels" by Agency insiders, had been compiled by his predecessor, James R. Schlesinger, who during his few months as DCI in 1973 set out to clean house.[2] It was, to say the least, a turbulent time for Colby—"one of the worst times in Agency history to become DCI," notes an Agency historian.[3] Colby found himself torn between a White House (under President Gerald R. Ford), which wanted him to be less forthcoming with lawmakers, and the Church Committee, which hounded him each day of the sixteen-month inquiry for more documents, more witnesses, and more candor. He attempted to strike a balance between the two demands, feeling that he had to be reasonably forthright with the Committee or else its members might react angrily by emasculating his beloved Agency. Convinced that lawmakers might even abolish the CIA if Colby failed to cooperate with the

investigation, the DCI decided to court the Church Committee and demonstrate to its members that intelligence could be made accountable to Congress. His mantra became another form of the CIA acronym: "Constitutional Intelligence for America," a slogan that seemed to many Ford administration officials as far too conciliatory to the Church panel. One of Colby's predecessors, Richard Helms—highly regarded among members of the CIA's Operations Directorate, where both Helms and Colby had pursued their intelligence careers—scorned Colby's deferential approach, arguing privately among colleagues that the best response to Congress was to hunker down until the storm subsided.

Perilous circumstances were nothing new to Colby, nor was controversy. As a young intelligence officer in World War II, he had joined forces with Norwegian insurgents in parachuting expeditions behind German lines to conduct sabotage operations against the Nazis in Scandinavia. During the Vietnam War, he had headed up Operation PHOENIX from 1968–71, a program designed to "neutralize" (read: apprehend or kill) the Viet Cong infrastructure in South Vietnam. The PHOENIX program led to the death of about 20,000 (Colby's estimate)—some say 60,000—suspected Viet Cong fighters or sympathizers. Colby maintained after the war that these deaths were a necessary part of the conflict, a byproduct of warfare. His critics, though, viewed the program as a massive assassination operation, anathema to American values.[4]

The critics had long memories. In 1979, when I was a staffer member with the House Permanent Select Committee on Intelligence and responsible for organizing a series of hearing for Representative Les Aspin (D-WI) on CIA relations with the media, then-retired Colby came to testify on this subject. Waiting for him in the back row of the hearing room were two young men with buckets of red paint they intended to throw over him in a protest against PHOENIX. The two were apprehended by Capitol Hill police before Colby arrived.

Just as Colby had performed well under fire in Norway and had responded calmly to the criticism rising from Operation PHOENIX, so did he steadfastly take on the task in 1975 of steering the CIA and the other intelligence agencies through the Charybdis of the Ford White House and the Scylla of the Church Committee. Certainly there are legions of intelligence officers who viewed him as too soft during that *annus horribilis*—even a turncoat—but many others inside and outside the intelligence profession admired his skill at navigating this tight strait in rough seas. As Frank Church's assistant during this time, I found Colby charming, bright, more or less cooperative in fulfilling document requests and calls for witnesses, and clearly correct about the need to work with Congress—or face the prospects of an infuriated investigative committee at a time when there was unambiguous evidence that the CIA and other agencies had improperly spied against innocent Americans exercising their First Amendment rights to protest against the war in Vietnam and in favor of the civil rights movement.

From the point of view of the Church Committee, Colby—however charming—was no pushover. For example, he strongly and successfully resisted the Committee's plan to hold public hearings on several covert actions that at the

time were (and remain) classified. He negotiated with Senator Church over every step of the inquiry and often persuaded the Committee to back away from some subjects that had nothing to do with illegal domestic espionage. On the subject of domestic improprieties, however, he was forthcoming and personally unhappy that they had occurred.

Colby was born on January 4, 1920, in St. Paul, Minnesota, the son of a U.S. Army officer who traveled with his family in tow to a number of assignments, including a stint in China.[5] A fine student, Colby went to Princeton University and graduated in 1940, then followed his father's footsteps into the Army, volunteering for active duty as a second lieutenant in August 1941. In 1943, he shifted over to the Office of Strategic Services (OSS), operating behind enemy lines in France as well as Norway. He earned a law degree at Columbia University after the war, practiced his profession briefly in New York (1947–49), and then went to work with the National Labor Relations Board in Washington, DC (1949–50). He joined the CIA in 1950. He rose through the ranks of the Operations Directorate, serving as chief, Far East Division, from 1962–67, before becoming director of Civil Operations and Rural Development Support in Saigon and head of the PHOENIX program (under the cover of the Agency for International Development) from 1968–71.

On returning to Agency Headquarters in Langley, he became the executive director and then comptroller from 1972–73 and—the plumb position for an operations officer, Deputy Director for Operations (DDO)—for six months in 1973. At the end of this brief period of work at the pinnacle of the clandestine service within the CIA, Colby was selected as the nation's top spymaster, the DCI, serving in this capacity from September 4, 1973, to January 30, 1976, in the midst of the Watergate and domestic spying scandals.

After his retirement in 1976, Colby authored two well-received books, his memoir, titled *Honorable Men*, and a book on his experiences in Vietnam titled *Lost Victory*.[6] Pointing to the French-language edition of the memoir, the CIA accused him of revealing classified information during his tenure as DCI about an intelligence collection operation that employed a deep-sea mining vessel, the *Glomar Explorer*, to salvage a Soviet submarine that had exploded and sunk in the Pacific Ocean near Hawaii. Colby agreed to pay $10,000 in an out-of-court settlement. For some, it seemed a petty retaliation by certain elements in the Agency against Colby for his "coziness" with the Church Committee. More conspiratorial still, some Colby supporters wondered if his death on a canoeing trip in 1996 might have had sinister causes. Police accounts, though, concluded that he had suffered a stroke or heart attack while canoeing in bad weather near his home at Rock Point, Maryland, with no evidence of foul play.

Five years before his death, as U.S. troops went to war in the first Persian Gulf War against Iraq, I sat down with him in his Washington law office on January 22, 1991, to discuss his career and the evolution of modern intelligence in the United States. Tanned and relaxed, he leaned back in his chair and smiled as I began the recorded conversation with questions about the Church Committee and the system

of intelligence oversight it had established in the aftermath of the 1975 investigation.

INTELLIGENCE OVERSIGHT

Johnson: Let me begin by asking you about this "grand experiment" we have been having in intelligence oversight. Do you think it has worked out all right?

Colby: I think it's worked out very well. Of course, there are glitches here and there, and some arguments. I think that Iran-*contra* was a direct violation of the deal, in both the respects of the refusal to send the finding over [to the congressional Intelligence Committees] on the Iranian part, and then coming up with the thesis that the Boland Amendment did not apply to the NSC [National Security Council], which was pure sophistry. I'm surprised [then DCI William J.] Casey didn't pick that up, because the Amendment very clearly says: "*any* agency engaged in intelligence activities." So if you engage, you're automatically included; it doesn't give you it by name. You will have that kind of thing forever: little things that happen here and there.

Johnson: The quality of intelligence oversight often seems uneven.

Colby: It's the same throughout the government. Sometimes people on the Agriculture Committees worry about what is happening in the Agriculture Department, and sometimes they don't. I think that's typical.

Johnson: Do you think that legislators tend to focus in when something goes wrong?

Colby: Oh, sure. That's the way the Hill works, which is fair enough; but they also look at things in the annual budget, which is down to a line-item thing. I remember one incident. Some people came to me with the idea of putting a bug out in one of the trust territories in the Pacific. I sent it up to the lawyers. I said, "Look, this is a trust territory. Is it outside the United States, or is it inside the United States?" And a lawyer came back and said, "It's outside." And I said, "Well, I don't think this will be worth a helluva lot, but okay, let's try it for three months and see what happens." Well, it leaked and Congress complained. I told them the operation had been there all along in the line-item budget. "It was there for you to ask about," I reminded them.

As I say, I never thought it was going to do a helluva lot of good, but I didn't want to put out the word throughout the Agency: "We're going to stop everything because of fear. So let's do the things. If they work, fine; if they don't, the hell with it."

Johnson: How do you develop comity between the branches?

Colby: I don't think you get comity. It's a deliberate separation of powers. I explained our government to a foreigner one time. I said, "Look, you're familiar with establishing a coalition government in your country. You establish a coalition, you agree on a program, and then everything more or less goes through because you have party discipline. You have to realize that in this country we have to establish a new coalition on each issue. There's no party discipline, so each issue has to have its own coalition." So it's consensus that you need, rather than comity.

There was a case here, I noticed in the paper, though it's a little fuzzy, that apparently before the attack in Panama [the United States invaded Panama in 1989] somebody came up with the idea of running a coup against Noriega. The possibility was mentioned in the *PDB* [*President's Daily Brief*]. This idea apparently got all the way to one of the [congressional oversight] committees, as was proper. The committee's members were being briefed on it, as they should have been. And it got into a discussion. If he's killed in the middle of the coup, is that an assassination? And it went back and forth, they mulled it over, and they finally decided not to do it. Instead [of a covert action], they [the first Bush administration] sent 24,000 troops and killed several hundred Panamanians; but I suspect that was the correct decision, because you'd still be hearing about the assassination of Noriega for the next hundred years—and you will not be hearing about the attack on Panama for the next hundred years.

Johnson: I think I've heard you say before that you would not even have ordered an assassination against Hitler before we declared war in 1941.

Colby: Before, no. After, it's an act of war; generals are just as subject to being killed as privates.

Johnson: What about assassinating Saddam Hussein instead of going to war against Iraq and inflicting perhaps thousands of casualties?

Colby: I basically think, no. You have to say, that's what happened in Panama [where the decision was made to arrest rather than kill the president, Manuel Noriega]. It's a tough moral issue. It's a very close call; but I think from the country's point of view, it's better to have a flat prohibition—except in war. And I don't mean to be fancy about war; I mean when our young men are dying, and the other country's young men are dying, then you can go after the top man.

Johnson: Are we likely to have another DCI in the future like Casey who does not appreciate oversight?

Colby: Yeah, sure.

Johnson: There is no way to get around that?

Colby: No, you just count on the tension in the constitutional system to work; and if it doesn't work and gets caught, then there's a back-up [judicial

proceedings] that's supposed to work for a while when someone goes off the reservation. It's like the laws against murder: murders take place even though we have laws, and we punish them when it happens.

Johnson: What about the question of access to information by Congress? Is the "sources and methods" argument a bit phony when it's brought up by the Agency in this context, as a means for avoiding the sharing of information with legislators?

Colby: I think it's pretty sincere, though they undoubtedly stretch it. Particularly on agent names, we did convince both [Senator Frank] Church [D-ID] and [Representative Otis] Pike [D-NY] to leave out the names [in their committee reports].[7] We pretty well got through that whole thing without names. It was critical. And the return on it was to be reasonably responsible. There's your comity; even when you're antagonists, you can have comity.

Johnson: Unless you're dealing with Otis Pike and some of his people?[8]

Colby: Oh, they were impossible!

Johnson: A lot of this depends upon personality.

Colby: Yes, of course it does—the character of the person and so forth. Back to sources and methods, the technological people—especially the cryptography people—are hyper about revealing anything, because it's just indoctrinated in them since Year One that if the other side learns you're reading their stuff, then they change their codes and there you are: you're lost. They just learn that from childhood. So that's why they get so upset. And when they have some new whizmo up in the sky that does something new and different, they want to keep a monopoly on the information. But you know, you can buy satellite photography now that is probably better than what we were guarding when I was DCI.

HUMINT

Johnson: If Congress were to examine the quality of HUMINT [human intelligence, collected by agents, as opposed to technical intelligence—TECHINT—gathered by satellites and other machines], wouldn't it have to get into some aspects of sources?

Colby: Yes, but you don't have to get into details. You see, you have undoubtedly seen some of the DDO [Deputy Directorate for Operations] reports and there's a source part: it's descriptive of the source, but it's also fuzzed enough so that you couldn't put it right smack on point. Now if you take the text and it says, "He [the agent] and I were in the garden and we had the

following conversation—" and you get that back to the originator, he knows damn well who was in the garden and you've got trouble.

Johnson: No member of Congress would want to know a name anyway, would he or she?

Colby: I don't think so. Once in a while there was a demand for a name of who was receiving subventions [money and other forms of remuneration from the CIA]. There were a few of those, where there were prominent people around the world who were getting help from us. They might also want to know who the intermediary was: "Are you sure these guys don't just pocket the money and run away with it?" This is a legitimate question, and you explain what you do to cross-check with some reasonable control; but quite honestly, you say, "I can't guarantee there isn't any waste here." Yes, it can happen; but still and all, we see the results and the activity that we're paying for, and therefore they [the legislators] seem reasonably happy about it.

CONGRESSIONAL ACCESS TO INFORMATION

Johnson: What about the timing of Congress's access to information?

Colby: I think Stan Turner [Adm. Stansfield Turner, DCI from 1977–81] said it about as well as anyone. He said at one point, when they were talking about this 48-hour stuff,[9] "Look, before Desert One, I had sent people over there [to Iran] in little planes to check out the desert to see whether it would hold the weight of a C-15. I am not able to look a young man like that in the face and tell him that I'm not going to tell ten congressmen [about the mission]; at the same time, I'm not going to lie to him. So, I need that kind of flexibility." I don't think you can write a law to cover it, but I think what you can say is [that] after the event, then Congress would have the right to review whether it was reasonable to withhold the information. In that case, they would have said yes.

But if it had been a jackass operation from the word go, then it might be that it would be reasonable to withhold that individual's involvement and the particular thing he did; but, in the same way, the Congress should have been informed that there was an overall program—as it probably was on the hostage rescue thing. I imagine there was some kind of briefing: that we are going to run some kind of operation some day, without any particular specifics. I would be surprised if [President Jimmy] Carter hadn't arranged for a few of the leadership [in Congress] at least to be brought into the fact that we're going to do something to try to get these people out.

Johnson: And if Congress doesn't like the rationale?

Colby: Then it can raise a fuss.

A GRAND CHARTER FOR INTELLIGENCE

Johnson: What do you think about the idea of a "Grand Charter" for Intelligence?[10] Has that gone the way of the dinosaurs?

Colby: That's gone. I was for it, I was for it. You could diddle with the details, but I've always been interested in getting intelligence a charter—a solid, statutory base—for its functions within the American government. The history of our intelligence is that we use it when we need it, and we throw it away when we don't. We throw away the organization. After World War I, after World War II—Truman tried to throw it away. It's sufficiently institutionalized now that I don't think you can throw it away, but that's part of what the charter proposal was about.

Johnson: I guess we're getting little pieces of the charter.

Colby: You've got little bits of it. I mean, this Agent Identity legislation, the "graymail" thing, the special court [for wiretaps]—that's a fabulous idea.[11] Star chamber! [Laughs.] It's so fascinating that the American citizen carries his constitutional protections with him even when he goes abroad.

FUNDING FOR INTELLIGENCE

Johnson: Does the CIA have access to money outside the appropriations process?

Colby: No.

Johnson: One example might be proprietaries . . .

Colby: We ran into that when we sold Air America when I was there. I've forgotten how much money we made off that—several millions of dollars, I guess. And I said, "Why don't we save the taxpayers some money? We've got this money; why don't we subtract it from next year's appropriation and use this?" I said, "Go up and talk to the Hill about it." They were interested, and then they ran into this general provision of law that says, "No agency of the government will spend nonappropriated funds." It was determined that the only thing one could do with that money was turn it in to the Treasury as miscellaneous receipts, and you had to get your full appropriation out of Congress, which is basically a good idea, because various intelligence services around the world have gotten into trouble by self-financing and going into their own deals, totally out of control, as the French did at one time.

Johnson: How do we know DCIs have indeed turned such profit over to the Treasury?

Colby: It's set into the rules. Now a proprietary will turn its own money over while it's still alive; in other words, you set up an air transport proprietary, you tell it to go out and do a certain amount of legitimate business so that you have cover for its other business. It'll turn over that basic capital.

Johnson: What if it makes huge profits?

Colby: Huge profits just build up; you can't take it anywhere. Now you may get a bigger airline, which is a little bit what happened to Air America. It got too big, in my mind.

Johnson: In the Iran-*contra* case, private American and foreign governments were willing to give money to pay for our intelligence operations . . .

Colby: Well, with respect to foreign governments, I don't know if they did or not; I can't answer that question.[12] There is an attempt in Congress now to write law that says, "Thou shall not urge a third country to do what you have not had authority from our Congress to do." President [George H. W.] Bush pocket-vetoed this, because he said it would stop you even from having diplomatic conversation with another country.

Johnson: That seems stretching it to me.

Colby: If you make the distinction that, "Why don't you help those guys?" and it's a direct relationship between those two; but "Why don't you give me money to help those guys?"—no, that's wrong. But I don't object to our government suggesting to the French government that it help the opposition against [Col. Muammar] Qaddafi [the leader of Libya].

Johnson: But should that be reported to the congressional oversight committees?

Colby: You don't have to report everything from a diplomatic exchange. It becomes a matter of whether it's an operation or whether it's just chit-chat. Again, how are you going to define that? If it's cooperation, then clearly you have to report it; but if it's just suggesting that somebody else do something useful, that's not quite the same.

WHITE HOUSE DETAILEES

Johnson: What about this question of detailees?[13] The argument that they run operations against the White House . . .

Colby: You wouldn't have a Director [DCI] very long.

Johnson: Where is the loyalty of these individuals?

Colby: It's like military officers. In my experience with military officers, you tell them what their chain of command is, and they salute. The same is true

with the CIA. Whether there's a little back-channel chatter on what's going on, I'm sure that occurs in the military and everywhere else; but in terms of someone using the position to spy for the Agency, I can't believe that. I would say that if you have a CIA career officer and you send him on TDY [temporary leave to serve as a designee] that you don't put him in the Peace Corps.

Johnson: And you don't make them Fulbright Scholars.

Colby: Right. Obviously we put people undercover all the time. Some of the political sections in the embassies are upset about this.

Johnson: You've spoken about the problem of "vanishing cover."[14]

Colby: Oh, it drives me up the wall. It's a serious problem. . . . So, obviously we've put people undercover, but in those situations they normally have a dual commitment; but what you're referring to is ostensibly, but not actually, a single commitment. I would have doubts that that would be at all feasible. There might be some informal chatter. And old friend calls up and says, "What the hell are you guys doing?" That's part of Washington.

MORE ON HUMINT

Johnson: Is HUMINT valuable?

Colby: It's one of those things, you can't afford to say no, because sometimes it can be. It's a very difficult subject. If in times of crisis, you have an agent in Baghdad, you would have a helluva time communicating to him right now. On the other hand, if he were reasonably close to the Revolutionary Command in the week before the crisis, he might have been able to give us a tip—that "He [Saddam Hussein] really is going [to invade Kuwait in 1990]. This is no bluff." I gather that was the analytical conclusion anyway. And of course, you go through years with nothing much happening, and then you cut off the relationship. We were in the process of closing the stations in El Salvador and Portugal just before [those countries] blew up; nothing had happened there for ten years! [Laughs.] And I was under a lot of pressure to squeeze down in personnel. So it's a tough subject. But I think that . . . well, when the Soviet Union was a monolith, then a little window into this section was quite valuable, because you had a reasonable case that what you saw there was probably typical of what was going on in the rest of the monolith.

Nowadays, with the Soviet Union spilling all over hell's half-acre and all sorts of voices coming from all sides, using a human agent doesn't have the same value. A human agent in the United States would be absolutely worthless [for a foreign intelligence agency], unless you want some highly technical subject. So, it's a tough subject; but I think you'll always have some, and

they'll pay off. And remember that the human agent is also available to somehow manipulate [a foreign government].[15]

THE DISSEMINATION OF INTELLIGENCE

Johnson: What can be done about the dissemination side of intelligence?[16]

Colby: Not very much. You do now pretty well disseminate it—you know, the estimates and that sort of thing to Congress. When [William H.] Webster [DCI from 1987–91] had to say that he thought the situation in Eastern Europe was irreversible, and [Secretary of Defense Dick] Cheney was trying to get a budget for Defense, Cheney was sore as hell. But it had its effect. It didn't have an effect on the administration's budget, but undoubtedly it's going to have an effect on the congressional budget.

Johnson: Where do you come down on the Sherman Kent argument versus those who think intelligence officers ought to be closer to policy makers?[17]

Colby: I think it ought to be closer—not supportive, but it has to be close enough to be related to what the hell is going on. When intelligence was sort of way over here in the early Nixon years [in other words, apart from the interests of decision makers in the government] . . . that was when Henry [Kissinger] was saying, "Oh, what is all this crap?"—it was true.

Johnson: Did [DCI] Casey carry this closeness too far?

Colby: I don't know that any allegation has been made that even Casey was warping the conclusions to fit the policy. I haven't heard that, one way or the other. Some guy [analyst] is always going to say that, if the DCI doesn't agree with him. That's one of the protections you have. The Agency is not a disciplined monolith. If you get something that does upset somebody, it'll come out sooner or later; then, you either defend it or admit that you shouldn't have done it. But that's a pressure point.

INTELLIGENCE COLLECTION AND ANALYSIS

Johnson: Are there any breakthroughs in methodologies for analyzing intelligence?

Colby: I know we were experimenting with some quantitative stuff. As you know, I did break up the Board of National Estimates, because I thought it was so generalist it was lacking in expertise. Then you need some protection against the Agency being the only source of opinion, and I think you get that through the [intelligence] community—having the arguments with the Navy, the Army, or whatever.

Johnson: Do we try to gather too much intelligence?

Colby: Not for a big nation. If I were Israel, I'd spend my time on the neighboring Arab armies and I wouldn't give a damn about what happened in China. We are a big power, and we've got to worry about all of the world.

COVERT ACTION

Johnson: Is covert action really all that useful?

Colby: I think it would be a mistake to get rid of it. Did we overuse it? Probably in some cases. But I think some of the major covert actions were very effective: the Laos case, Western Europe.

Johnson: What about Afghanistan? Was covert action effective there [in the 1980s]?

Colby: Afghanistan, certainly. Even you might say Cambodia. I don't know about Angola. All that was part of the Cold War, the containment policy. The Bay of Pigs was a disaster, of course. But what if it had worked?

DCI–WHITE HOUSE RELATIONS

Johnson: What about DCI access to the White House? Can you mandate it?

Colby: I don't think you can mandate it. I think Casey had too much [during the Reagan years]. I think [Richard] Helms had about the right amount with [President Lyndon B.] Johnson—the Tuesday "lunch group," you know. He was in the circuit. He was quite meticulous about not taking a policy position. But he was still in on the President's agonizing, so he knew how to manipulate the machinery, too. You either support the President, or offer advice that he was on the wrong track. I think the Pentagon Papers are quite a tribute to Helms; you know, Johnson was not the most patient guy in the world.

Johnson: What about your own access?

Colby: I had very little. I had all I wanted to [National Security Adviser] Brent [Scowcroft]. I was on the phone to him every day or so. [Secretary of State] Henry [Kissinger] I'd see fairly frequently. President Nixon was such a retired fellow that you didn't see him very much—though [on those occasions when he did talk to me] he would listen and often disagree, which was fair enough. [President] Ford was more regularized. He'd have the meetings in the NSC on the various issues, so you'd prepare for those. He wasn't very informal on that sort of thing.

Johnson: So Nixon wasn't very interested in meeting with DCIs?

Colby: No, I think one time he called me up and asked me what was happening in China—just out of the blue.

Johnson: Ford didn't seem to treat you well.

Colby: I understood what his problem was. He was taking such a pasting on [intelligence] issues [in 1975–76] that by stepping in and putting his own man in [in other words, Colby as a replacement for DCI James R. Schlesinger]—and, remember, one of the motives of this thing was to conceal the dumping of a vice president [Spiro Agnew]; that was behind the scenario—and, of course, Ford never understood Schlesinger, so he just threw me in as an also-ran.

COUNTERINTELLIGENCE

Johnson: What about the Nosenko case?[18] Did [CIA Chief of Counterintelligence James J.] Angleton order that confinement?

Colby: No, apparently he did not. Apparently there is even some doubt that he had anything to do with the actual confinement. I don't know. This was before my time. Obviously, he was in the loop of the whole thing, but what he knew about the confinement, I don't know. And I can't name who did. It's the thing that scared me the most. The assassination of a foreign leader may be dumb, but to take someone and put him in jail in the United States . . . what the hell happened to habeas corpus? This is pretty fundamental. For an intelligence agency to do that in this country—Jesus! Though I gather Nosenko accepted it as "So what's new?" [Laughs]

Johnson: What are the chances that the CIA is currently penetrated at the top? Especially by the Soviets.[19]

Colby: It would be my guess, no. I can't say no absolutely. If it is, you don't know. We did have Alger Hiss, and those punks at various levels; then that Chinese fellow at FBIS, which was a surprise to me.[20] I don't say it's impossible. I just don't think so. Frankly, I think we would have heard about it by now. The big thing we have, which the British did not have, was the security clearances and the polygraph. Now I don't believe in the polygraph either, but it sure as hell helped us. My security people told me that, faced with the polygraph, people told us things that caused us not to hire them. As far as I'm concerned, it paid for itself right there.

Johnson: But the polygraph is no fool-proof system?

Colby: No, and the real weakness was, once you get in [as an employee of a U.S. intelligence agency], there wasn't enough periodic checking.

CIA OVERSIGHT

Johnson: How well has the IG [Inspector General] system worked inside the CIA?

Colby: Well, it's like the IG in the military. They do periodic inspections, and they're a useful investigating team for the director if something is strange. He just tells the IG to look into it. It's a bureaucratic mechanism to get something done; but as a great safety valve, I'm not so sure—any more than the IOB [Intelligence Oversight Board, a panel for intelligence accountability established in the White House in 1976]. I mean, it's there, but I don't think [it always works well]... Congress is the real safety check.

Johnson: And the press?

Colby: And the press certainly; and the feeling that if something is wrong, people will make it known. I have no idea how many sources someone like Seymour Hersh [a *New York Times* reporter] has, but it must be dozens; they must be all over the place. And so if anything is seriously wrong, it'll come out.

Johnson: Some say the FOIA [Freedom of Information Act] is the most important source of oversight.

Colby: Well, in a way, but now they've exempted the operations files from that—for good reason; it was just a useless exercise. I think it's the press and Congress, and the sort of the traditional feeling that if something is bad you should do something about it. The normal, good, loyal American citizen will think.

THE ROLE OF THE DCI

Johnson: Is the DCI biased toward the CIA?

Colby: If anything, the DCI is inclined to take kind of a position showing that he is not biased. He obviously knows [the CIA] better; his contact with the rest of the services is episodic.

Johnson: Do we need a more powerful DCI?

Colby: I think you've got to have a very close, coordinating mechanism. We use to have weekly meetings of the U.S. Intelligence Board, at which you get the senior representatives of each of the agencies there. This was very useful, because you could argue things out, you know, discuss them. And it was helpful not only in the substantive discussion of what's happening in Argentina (if you're making an estimate or something), but also in the practical sense—you

know, how many of these goddamn satellites do we really need? Do we need fifty, or do we only need ten? And you work through those things. You do a lot of staff work beforehand—each agency does.

Johnson: As DCI, does one feel in control of the Agency?

Colby: I think you have to work at it, and that means you have to use your chain of command. You also have to have some independent reporting as to what's going on. You get out of your chair and go out and look . . . talk to people. It's like running General Motors. You're not going to run everything in General Motors; but you can have the auditors and you have the other people to keep it under some semblance of control. I think that business of being in control also has something to do with the attitude of people. When George [H. W.] Bush came into the office [as DCI, following Colby in 1976], there was this wonderful story about him. Three days after he got there, they were having this meeting and somebody said, "Well, there's a story in the press that says we did this or that." And Bush said, "What are they trying to do to us?" *Us* after three days. [After that], he had the place in the palm of his hand.

Turner was at the opposite end. He was afraid of them.

I use to say that one should have an outsider [as DCI], with an insider deputy, because the inside deputy will give the local knowledge and the outsider will give you a little of the independence. You take somebody who comes up through the career [ranks of the CIA]; you're ideas are shaped by what you did during the career. I always thought the best director I ever knew, including myself or anyone else, was John McCone [DCI from 1961–65], and he was an outsider. His first deputy was an outsider, too, General [Charles Pearre] Cabell; but there were other professionals who ran the different directorates.

Johnson: Why was McCone so good?

Colby: He was just such a consummate manager. He would say, "I want this done by tomorrow morning. I want this. I want this. Where is it?" No softness. "Goddamn it, let's get it done!" He had the place totally excited. He'd go down to the White House, and write up six questions on a piece of paper on his way back in the car. He turned this over to [the dean of the CIA's intelligence analysts] Sherman Kent or whoever and say, "I want these answered by 8 o'clock tomorrow morning: 'If we do this, what will China do? If we do that, what will the Soviets do?' Answer those questions." And, of course, they [the analysts] loved it. Absolutely loved it. They worked like hell, and he would then go in and make no bones about what he thought about it [the analytic products].

Johnson: We've drifted away from the notion that we ought to have a military person as DDCIA [deputy director of the CIA, the second in command at the time after the DCI].

Colby: Yeah, we use to feel we had to, but I don't think you do now. I think the reason you don't need to now is that the DIA [Defense Intelligence Agency] fulfills that function—giving senior status to the military. It use to be we thought that to keep some semblance of comity with the military that we had to have a military deputy [at the CIA, as deputy to the DCI]. This is not so important now.

COLBY'S SELF-APPRAISAL

Johnson: What were your most important contributions as DCI?

Colby: Well, I think the thing that will last longest is this constitutional thing—just getting through it alive [the Church Committee inquiry and related investigations]. I think that is the longest term effect that I had. Oh, I fooled around with some of the internal machinery. The other thing I think I started, and Casey finished, was the NIO [National Intelligence Officer] system, which led to the reorganization of the analytical side. Sherman Kent points out in his book, *Strategic Intelligence,* published in 1949 by Princeton University Press, that you organize intelligence either by subject or by area. He said there are arguments for and against both ways. He said that, on balance, "I think it ought to be area," but he wasn't very strong about. So we organized it by discipline: political, economic, scientific, military, all those.

And I got in and I remember one time asking to see some people talk about China, and, Jesus, fifteen people came in! And I realized I was the only central figure of all of those fifteen. I said, "I can't do this for China, for the Soviet Union, and for everything else—this is crazy." We had this Board [of National Estimates], which I had doubts about anyway; so I set up the NIO system. I considered whether we should go ahead and try to reorganize the analysts; and I said, "Christ, we have enough turmoil around here: no, not now."

Casey did, and he did it very quickly after he went into office; he just reorganized. And of course, I often wondered why the hell we did it this way, until somebody pointed out, "That's the way you organize universities"—which have a different function than intelligence. Intelligence is supposed to react to problems and opportunities, and they come largely in geographic terms—not in economic terms or political terms. They come by geographic area.

Johnson: Say, "What are we going to do in China?"

Colby: Sure. This was one of the reasons—that inadequate organization in the early stage—that analysts didn't play a bigger role during those twenty-odd years, because they were all divided up. I remember there was a time, when I was chief of the Far East Division, I was the one going to talk to State or the military about the Far East—not the analysts. I never read NSA [National

Security Agency] traffic, yet here I would be representing intelligence in a meeting on policy, and I was the worst one to do it; it should have been an analyst. Now that is very much the case: the chief of China, he's the guy who goes to the White House meetings for the director.

Johnson: Can you recall any mistakes you made as DCI?

Colby: Obviously, the Yom Kippur War we didn't distinguish ourselves on.[21]

Johnson: I guess there will always be surprises.

Colby: There is that thesis. But my contention—in a way, a mental game—is that if intelligence does its work well and anticipates some problem arising and communicates this to policy makers; and policy makers act so that the thing does not happen in a bad way, but happens in a good way, intelligence turns out to be wrong—but wrong for the right reasons. So I think your record is: How many things do you get policy to move on, and how few bad surprises? I use to say, "I don't mind good surprises, but I don't want any bad surprises." And I think that is a legitimate demand. But you should be braced for the bad. On that Yom Kippur one, we just had convinced ourselves that it didn't make sense. And it didn't! But . . .

LOOKING BACK ON THE YEAR OF INTELLIGENCE

Johnson: Would the CIA have been in big trouble if you hadn't cooperated with the Church and Pike Committees?

Colby: I thought so. I was walking along by the Library of Congress one time—five, maybe eight, years ago—and this fellow who was counsel for the House [Appropriations] Committee crossed the street to me, and he said, "I just want to tell you something. I heard that you thought that, if you weren't cooperative with Congress, they would have gone out to destroy the Agency. I just want to tell you, you're absolutely right. We would have." They were out for blood, so I was throwing things at them, trying to be *reasonably* responsive and trying to protect the Agency. And I considered, really, the greatest victory in that was the Church Committee report, which is not a bad report, it really is not an unbalanced report. It's a little more sanctimonious than I'd like to have had; but when they came down to that part about covert action, I thought we'd come home free—you know, we shouldn't use it very often, but we shouldn't dismiss it. I was really a little surprised, because I thought we'd have a little more antagonistic [report]. The Pike Committee report was useless; but the Church Committee report, if you read it through, hangs together pretty well.[22]

ECONOMIC ESPIONAGE

Johnson: Should the CIA be more involved in economic intelligence and assisting American industry?

Colby: My answer to that is it certainly ought to be more active in the economic analytical area, because economics is going to be a big subject for the next decade or so. It's a major subject and CIA has excellent capabilities in this area. Collection? Overt collection, fine, no problem; covert collection, very rarely and only when there is some strategic reason for it. If you're engaged in illegal espionage in another country, you're entitled to do it for your security; but you really don't [if your objective is simply] to save a few bucks. You don't need to use satellites to count Toyotas.

And what do you do with it [the intelligence]? Suppose you have the information that Toyota is going to come out with a new model, and you got it through a secret penetration—what do you do with it? Both I and Stan Turner experimented with putting out some [public] economic reports, and it was hopeless. It would be met with: "Oh, this is spying!" And it had nothing to do with spies at all. Either they overbelieved it, or just laughed about it—giggled. We did work up a set of relations with the other departments, comparable to the one we have with the Defense Department, where we funneled the information over to Commerce, to Treasury, to Agriculture, I guess, wherever else. Then they absorb it into their business, and they put it out. And they don't just put it out to Ford; they can't. They put it out evenly; and that means it has to go to the foreigners, too, who are by now smart enough to know how much information there is in this city.

But I think the risk factor is such that I would be sort of dubious about this. I won't say never—you know, never say never. But it would have to be something very vital. And of course, controlling the illegal diversion of military related equipment, that sort of thing, proliferation of weapons, all that sort of thing, that's fine, sure.

THE FUTURE OF INTELLIGENCE

Johnson: Will the future mission of U.S. intelligence change much?

Colby: Not a helluva lot. [Colby referred me to a piece he had written recently on intelligence.[23]]

Johnson: Thank you for spending this time with me.

Colby: Thank you.

NOTES

1. For an account of this period, see Loch K. Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (Lexington: University Press of Kentucky, 1985).

2. The "jewels" included details on CIA assassination plots against foreign leaders, drug testing on unwitting subjects, opening the mail of selected American citizens without a warrant, and spying on Vietnam War protesters.

3. David S. Robarge, "Intelligence in Recent Public Literature," *Studies in Intelligence 47* (2003), available at https://www.cia.gov/csi/studies/vol47no4/article07.html.

4. See, for example, Dale Andradé, *Ashes to Ashes: The Phoenix Program and the Vietnam War* (Lexington, MA: Heath, 1990).

5. For a biography, see John Prados, *Lost Crusader: The Secret Wars of CIA Director William Colby* (New York: Oxford University Press, 2003).

6. William E. Colby with Peter Forbath, *Honorable Men: My Life in the CIA* (New York: Simon & Schuster, 1978); William E. Colby and James McCargar, *Lost Victory: A Firsthand Account of America's Sixteen-Year Involvement in Vietnam* (Chicago: Contemporary Books, 1989).

7. Representative Otis Pike (D-NY) headed up a panel of inquiry in the House of Representatives during 1975. By mutual agreement, the Church Committee focused on questions of intelligence improprieties at home and abroad, whereas the Pike Committee examined questions related to the quality of intelligence collection and analysis.

8. The Pike Committee engaged in a running battle with Colby and the Ford administration during its investigation, whereas the Church Committee attempted to have a more cordial relationship, based on the notion that you catch more flies with honey. The vitriol between the Pike panel and the administration led to the failure of that committee to win the trust of House members, and the investigation faltered in a whirlwind of dissension inside the panel and with the administration. See Frank J. Smist Jr., *Congress Oversees the United States Intelligence Community, 1947–1989* (Knoxville: University of Tennessee Press, 1990).

9. According to the Hughes-Ryan Act of 1974, covert actions were to be reported to Congress "in a timely fashion," which the floor colloquia preceding passage of this law seemed to define as within two days.

10. In 1976–78, the Senate Select Committee on Intelligence attempted to draft an omnibus charter for intelligence to replace the sketchy details of the National Security Act of 1947. This proposed law became long and convoluted and eventually collapsed under its own weight, with the help of lobbying against it by the intelligence bureaucracy. See Loch K. Johnson, "Legislative Reform of Intelligence Policy," *Polity* 17 (Spring 1985), pp. 549–73.

11. In 1982, Congress passed the Intelligence Identities Act to protect intelligence officers and their agents against the disclosure of their names by outsiders, whether newspaper reporters or enemies of the United States seeking to destroy the CIA and the other intelligence services. Four years earlier, in 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA)—a major Church Committee recommendation—that required judicial warrants for intelligence wiretaps and other forms of surveillance, instead of just an order from a president or some other executive branch official. The term "graymail" refers to a threat by a defendant in a court proceeding to expose intelligence operations or other classified information if prosecuted. During the 1980s, the executive

and legislative branches worked together on procedures to conduct trials related to intelligence without exposing classified information.

12. For evidence that money was raised from foreign nations, see Senate Select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition and House Select Committee to Investigate Covert Arms Transactions with Iran, *Hearings and Final Report* (Washington, DC: Government Printing Office, 1987).

13. Detailees are individuals loaned to the Executive Office of the Presidency from various government agencies around Washington for employment by the President without cost to the White House.

14. See William E. Colby, testimony, "The CIA and the Media," *Hearings*, Permanent Select Committee on Intelligence, U.S. House of Representatives (Washington, DC: Government Printing Office, 1979).

15. That is, human agents don't just gather intelligence, they can also engage in covert actions as well as counterintelligence deception and penetration.

16. This refers to the connection between intelligence professionals and policy makers. Transferring intelligence from the former to the latter is rife with difficulties, perhaps the most important being the distortion of intelligence by policy makers to suit their own political needs.

17. Yale University history professor Sherman Kent served in the CIA as a high-level analyst and argued consistently for a strong barrier between analysts and policy officials, as a means for preserving the neutrality and integrity of analysts (see the chapter by Harold M. Greenberg in Volume 1 of this series).

18. Yuri Ivanovich Nosenko was a Soviet defector banished to the CIA's training facility at Camp Perry (The Farm) in Virginia, where he was confined and interrogated at length to test his bona fides. For one account, see Edward Jay Epstein, *Legend: The Secret World of Lee Harvey Oswald* (New York: Reader's Digest Press, 1978).

19. We now know that Aldrich H. Ames was a Soviet/Russian mole at the time of this interview, as was FBI agent Robert P. Hanssen.

20. Larry Wu-tai Chin became a translator for the United States on Okinawa and later gained employment at the CIA as a translator for its Foreign Broadcast Information Service. See Ronald Kessler, *Inside the CIA* (New York: Pocket Books, 1992), p. 155.

21. This was an unpredicted war between Egypt and Israel in 1973.

22. For the Church Committee Report, see Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Final Report*, Sen. Rept. No. 94–755, 6 vols., 94th Congress, 2nd sess. (Washington, DC: Government Printing Office, November 20, 1975). The Pike Report leaked to a New York City magazine: "The CIA Report the President Doesn't Want You to Read: The Pike Papers," *Village Voice*, February 16 and 23, 1976. A third investigation in 1975, this one by the White House under the leadership of Vice President Nelson Rockefeller, was expected to whitewash the intelligence abuses, but instead produced a hard-hitting report focused on illegal CIA domestic operations; see Commission on CIA Activities within the United States, *Report to the President* (Washington, DC: Government Printing Office, 1975).

23. William E. Colby, "Intelligence in a New World," *Mediterranean Quarterly* 1 (Fall 1990), pp. 46–59.

4

THE BRITISH EXPERIENCE WITH INTELLIGENCE ACCOUNTABILITY

MARK PHYTHIAN

THIS CHAPTER ASSESSES THE BRITISH EXPERIENCE WITH intelligence accountability through a consideration of the principal mechanism that exists to provide for this—the Intelligence and Security Committee (ISC). In discussing the British experience with intelligence accountability, we are looking at a country whose principal internal security and external intelligence organizations—the Security Service (MI5) and the Secret Intelligence Service (MI6)—trace their origins back to 1909 but whose peacetime existence was only formally acknowledged in the late 1980s and early 1990s. Then, in the wake of a succession of intelligence-linked exposés and in the context of the end of the Cold War and the intrusion of European law into the domestic polity, the Conservative governments of Margaret Thatcher and John Major finally introduced legislation formalizing their existence.

THE EMERGENCE OF OVERSIGHT

A string of revelations and allegations during the 1970s and 1980s created a momentum for greater accountability of the security and intelligence agencies, albeit one that lagged behind similar debates in the United States, Canada, and Australia. The motor driving these concerns was the widespread belief on the Left that in guarding against domestic subversion, MI5 was monitoring and interfering with legitimate political dissent. Left-wing critics argued that MI5 saw its primary allegiance as being to the Crown rather than the elected government of the day. There were suspicions that this extended to undermining Labour governments, reinforced by the revelations contained in former MI5 officer Peter Wright's

memoir *Spycatcher*. There were other dimensions to the damage done to the reputation of the security and intelligence services during this period. The public exposure in November 1979 of Sir Anthony Blunt, surveyor of the Queen's Pictures and pillar of the establishment, as a former Soviet spy was quickly followed by the Prime and Bettaney espionage cases, all of which provided fertile ground for Wright's claim that former MI5 Director-General Sir Roger Hollis had been a Soviet spy. By the time of Paul Foot's 1989 book, *Who Framed Colin Wallace?*—at its core an account of the "cowboy" era of military intelligence in the laboratory that was Northern Ireland in the early 1970s—it seemed that there was a reservoir of security and intelligence intrigue and scandal that was in no danger of running dry.

While all of this created heightened parliamentary concern, the existence of what Tony Geraghty has termed the "very public war" in Northern Ireland served as a disincentive for government to act.[1] When Parliament did probe, former ministers were hardly reassuring. For example, when former Prime Minister Jim Callaghan gave evidence to the Treasury and Civil Service Committee in 1986 and was asked if he was satisfied that the agencies were sufficiently accountable, he replied:

> I am not sure what its accountability is to Parliament, I am not sure about ministers. I find it a difficult question to answer, I really do. They are run . . . as separate departments. They are not in the Minister's office, as it were, not in his headquarters. There is, therefore, all the difficulty of physical separation. When the Minister has to up sticks to ask questions and go somewhere else, that makes for remoteness. There is not immediate day to day closeness. Some Ministers do not want to know a lot: Home Secretary or Foreign Secretary, Prime Minister, others want to know a great deal about what is going on. I am going to give you a very unsatisfactory answer, I do not know. I am certain there must be a very high degree of responsibility among those who serve in MI5 or MI6 because they have great powers . . . and I think the ethos of those particular services is probably as important as the degree of accountability that you can visit upon them. I am very, very mixed up about this, I do not think I can help you with this.[2]

The most pressing impetus to act from the British government's perspective (although it did not concede this at the time) arose from the impact of European law on the British polity, in particular the European Convention of Human Rights (ECHR). Having fallen foul of this in 1984, the government enacted the Interception of Communications Act the following year. When former MI5 officer Cathy Massiter revealed that future Labour government ministers Harriet Harman and Patricia Hewitt had been placed under surveillance as a consequence of working for the National Council for Civil Liberties, at that time classed by MI5 as a subversive organization, they prepared to take their case to the ECHR. The prospect of further adverse rulings led to the 1989 Security Service Act.

This established MI5 on a legal footing. It created a commissioner, "a person who holds or has held high judicial office," who would review the Home

Secretary's exercise of his powers in signing warrants allowing for interference with private property and produce an annual report for the Prime Minister, who would lay it before Parliament after removing any material considered "prejudicial to the continued discharge of the functions of the Service." The act also created a three-member tribunal to investigate complaints about MI5 from the public which, like the commissioner, had access to MI5 records and personnel. The tribunal would (in conjunction with the commissioner where allegations of property interference were involved) establish whether MI5 had conducted investigations into a complainant and, if so, establish whether the grounds for doing so were reasonable. If the tribunal found against MI5, it could order that any records relating to the complainant be destroyed, further investigations ended, and compensation paid. Out of over 100 cases investigated by the tribunal in its first three years of operation, it did not find for the complainant in a single case. Nevertheless, the commissioner, in his 1992 annual report, suggested that the very existence of the tribunal had acted as a spur to MI5 adopting a more cautious approach to warrants and surveillance.

In mid-1992, Prime Minister John Major, then embarked on a wider "open government" drive, broke with tradition by admitting that MI6 actually existed and undertaking to put it on a statutory footing. Briefings to journalists at this time suggested that parliamentary scrutiny of the services was unlikely to be a feature of this opening. However, when the Intelligence Services Bill was unveiled in 1993, tacked on to the end was provision for a form of parliamentary scrutiny of MI5, MI6, and the Government Communications Headquarters (GCHQ).

Why did Major move to introduce an oversight body at this time? There is no doubt that the end of the Cold War created a political space that made this possible. At the same time this left politicians feeling bolder about removing some of the secrecy surrounding MI5 and MI6, it also affected these organizations' own view of the desirability of a limited degree of accountability. There was a general expectation that the end of the Cold War would bring with it a peace dividend, with clear implications for defense budgets. The intelligence agencies could expect to face similar pressure. In this context, it was felt that agreement to some form of scrutiny was necessary in retaining public confidence and protecting the U.K. intelligence budget (in 1992, £185 million). Moreover, the more perceptive intelligence managers may have appreciated that if oversight was increasingly inevitable, it should be accommodated rather than resisted. After all, scrutineers could also become advocates. They also faced the prospect of a future Labour government seeking to introduce more far-reaching reforms than the agencies were comfortable with. The Labour Party's 1983 election manifesto had spoken in terms of the "now widespread concern about our security services" and committed a future Labour government to introducing legislation that provided for oversight by a select committee, a prospect which must have caused some concern in the agencies. Reinforcing such arguments in favour of cooperation would have been the feedback from foreign counterparts subject to oversight, offering reassurance that it could be accommodated.

Moreover, in searching for a post–Cold War raison d'être, MI5 had assumed the lead role in combating terrorism in Northern Ireland (a role previously occupied by the Metropolitan Police Special Branch) and as such were under some pressure to make themselves as accountable for their part in this as the police had been. At the same time, allegations continued to emerge that strengthened the case for oversight—for example, those emanating from the Scott inquiry into the arms-to-Iraq affair, and concerning the role of MI5 during the 1984–85 miners' strike. Finally, MI6 reportedly took a more relaxed view of the prospect of oversight than MI5, on the basis that its operations abroad were likely to be of less concern to MPs than the domestic operations of MI5, which carried greater concerns over civil liberties. Crucially, legislating from a position of relative strength, rather than being driven by some scandal, allowed the government and agencies to control the agenda. A key dimension of this was the idea, to quote Foreign Secretary Douglas Hurd, that "the past is another country" and not one that the oversight body would be invited to explore.

THE INTELLIGENCE SERVICES BILL

The Intelligence Services Bill included provision for the creation of a committee of six parliamentarians (increased to nine—the only alteration made to the draft bill), hand-picked by the Prime Minister, who would meet in closed session and produce reports for the Prime Minister, who would lay them before Parliament after removing material considered prejudicial to the activities of the agencies. Hence, it was accountable to the executive and only through the executive was it accountable to the legislature. This arrangement would be a continual source of soul searching and debate as to whether the committee should not be a select committee of Parliament, directly accountable to the legislature. To coincide with the introduction of the bill, the head of MI6, Sir Colin McColl, made an unprecedented public appearance to welcome the move toward greater accountability but also reassure former, current, and prospective agents that "Secrecy is our absolute stock in trade. It is important to the people who work for us and risk their lives that we remain a secret service. When the Central Intelligence Agency went open in the 1970s it worried a lot of their people. I want to send our people a signal that we are not going to open everything up."[3]

McColl may have welcomed the bill, but the Labour opposition did not, arguing for scrutiny by a parliamentary select committee rather than the proposed hybrid. As Jack Cunningham, leading for the opposition, put it:

> It is proposed that the committee should not report to Parliament but to the Prime Minister. I do not regard that as parliamentary scrutiny or oversight, because the Prime Minister has the right to veto sections of its report—I call it prime ministerial oversight and scrutiny. If we are to have an effective parliamentary watchdog to oversee such matters and to probe and scrutinise, it should report to Parliament. It cannot legitimately be called a parliamentary committee unless it does so.[4]

Future members of the ISC were among those who expressed concern over the proposed form of oversight. Labour MP John Gilbert called it "far more timid than necessary." He was one of several MPs who could not see that the government had made the case for not granting the proposed oversight committee select committee status, arguing that the existing select committee practice of "sidelining" (i.e., removing) sensitive material would apply. The advantages to the government, it was argued, lay in controlling the timing of publication of the report, and that the proposed committee would not have the same powers as a select committee to send for persons and papers. As future ISC member Allan Rogers put it, "The committee will be a charade, a pretence at accountability."[5] In general, the opposition made it clear that while voting for the bill, they favored select committee status. It would be two years later, with the increasing likelihood that they would form the next government, before the Labour Party began to distance itself from its earlier enthusiasm for genuine parliamentary oversight.

In response to fears that the proposed committee would be toothless, Willam Waldegrave closed the debate by emphasizing the powers that it would possess:

> The committee will be involved in very secret areas that have never before been shared with others outside the Secretary of State's responsibilities. . . . The committee will not only deal with high-level policy in a broad-brush way; it will be able to examine the actual tasking, the money and the organisational structures. The committee will be fully trusted, and fully inside the secret wall. I believe that the result, while it will not establish within the House the parliamentary accountability that . . . we believe would be extremely difficult to organise, will be to spread the reassurance that senior, trusted people on both sides of the House share the secrets of the services, and have a formidable power to cause trouble for the Government. Somebody asked earlier where the teeth were. The teeth consist of the fact that the committee . . . will have the right not to publish stuff that would damage national security—which it would not want to do—but to write a report saying, "We believe that things are not being handled properly, and that Ministers are not responding properly." No Government . . . would want to risk such criticism.[6]

THE ISC UNDER TOM KING, 1994–2001

Nevertheless, the ISC would first of all have to discover that things were not being handled properly, and there remained concerns about its ability to do so. The final Intelligence Services Act stated that the ISC's requests for information would not be met if that information was deemed "sensitive" (and "sensitive" was broadly defined) or because the Home or Foreign secretary "determined that it shall not be disclosed." As with the 1989 act, a commissioner and tribunal were created. The separate tribunals have since been supplanted by a single tribunal under the terms of the Regulation of Investigatory Powers Act 2000, introduced to keep pace with advances in European law. In his brief annual report, the commissioner registers the number of warrants issued in a confidential

annex while openly recording the number of complaints investigated by the tribunal, and the number upheld following investigation, usually none.

The ISC's first chairman was former Conservative Secretary of State for Defence and Northern Ireland Tom King, and the committee featured a Conservative Party majority. Its first report was an eleven-paragraph interim report published in May 1995, reporting that "In general terms, we have been encouraged by the openness of the intelligence 'insiders' that we have come into contact with thus far, and in particular by the helpful approach of the Heads of the Agencies themselves."[7] In an eleven-paragraph report, the inclusion of the preambular "in general terms" was not without significance. In terms of the Committee's approach, the report noted that it would "concentrate on major issues rather than, for example, be dawn into every individual intelligence item of current excitement—unless they are of such significance and relevance as to merit exceptional consideration and report to you." The framing of the Committee's interpretation of its mandate inevitably involved a tussle over the question of investigating allegations of past abuses. An attempt by Allan Rogers to raise the question of the agencies' relationship with Soviet defector Oleg Gordievsky, in the context of his contemporaneous allegation that former Labour Party leader Michael Foot was regarded by the KGB as an "agent of influence," were defeated inside the Committee, with Lord Howe echoing Douglas Hurd's earlier intervention and arguing that the ISC should not involve itself in "political archaeology." However, in the United States, Canada, and Australia, the question of past abuses or scandals was among the first to be investigated by the newly formed oversight committees. Having decided that the past is another country and interpreted its mandate as involving broad, strategic policy questions, in its first years of operation the ISC focused on the implications for the agencies of the changed post–Cold War world. Its second report, nine paragraphs long, concerned the decision to move MI5 into the fight against organized crime. Its first annual report was completed in December 1995 and published in March 1996.

There is no doubting the industry of the individual committee members in getting to grips with their task, nor the learning curve they faced. This first annual report revealed what became a pattern of at least weekly meetings and visits to the agencies and abroad (although the agencies have always stressed the limited utility of overseas experiences with accountability, instead emphasizing the unique character of MI5 and MI6). On the basis of its early experiences, the ISC felt able to reassure the Prime Minister that it considered its structure appropriate to the task. However, it would not be long before it requested the addition of an investigative capacity to assist it in its work.

One fundamental early aim of the ISC was to establish the confidence of the agencies themselves. King would subsequently allude to the initial Australian experience with intelligence oversight, wherein what he called the "awkward squad" was selected to sit on the oversight body, and consequently enjoyed little cooperation from the agencies. The ISC sought to reassure the agencies that any

information they shared with committee members would be handled securely. In return, the ISC was keen that in turn the agencies

> Understand our needs and are sufficiently frank and open with a new oversight body with whom they have previously not had to relate. These mutual concerns must be met if the Committee is to command the confidence of parliament and the public. This is an essential foundation for our work, particularly if we were at any time required to deal urgently with some specially sensitive or difficult issue.[8]

In comparing the U.S. intelligence agencies' legal obligation to keep their oversight committees informed of their activities with the U.K. agencies' much more limited legal obligation to respond to ISC requests for information, the report later observed that the ISC "does expect to be kept properly and promptly informed." How fully the ISC succeeded in this area is an open question. Nevertheless, it is worth noting that this expectation represented something of an attempted expansion of its role—the Act was silent here. Similarly, its first annual report adopted an expansive interpretation of its financial oversight remit, arguing that this extended to "the clear responsibility to ensure that the Agencies have access to adequate resources for the tasks they are asked to undertake,"[9] and not just how cost-effectively such resources were used.

The second annual report, for 1996, was completed in December 1996 and published in February 1997. This reported that the Committee had faced the first challenges to its decision to focus on major issues (rather than feel obliged to address each and every controversy that might arise) in allegations concerning Menwith Hill and, separately, the alleged surveillance of a meeting between MPs and members of Sinn Fein inside the Palace of Westminster. Having asked the agencies about these matters, "we received . . . categorical assurances, which we accept, that the stories were without foundation."[10] Having no wider investigatory capability, the Committee had little option but to do so.

The third annual report was completed at the end of July 1998, a full nineteen months after the previous one, the intervening period disrupted by the election of a Labour government in 1997 and the subsequent reorganization of the ISC to reflect political retirements and the parliamentary dominance of the Labour Party. King remained as chair of the Committee, reflecting the desire of the Labour government to reassure the agencies that the 1983 election manifesto was long forgotten. With this new membership, the ISC came to see itself as having more of a public education role, opening its third annual report with a lengthy overview of the recent history of the agencies and the evolving nature of the threats they countered. The Committee assured the Prime Minister, Parliament, and public that these new challenges were "real enough" and not "invented to justify the Agencies' continued existence," as some critics had asserted, and moreover that "intelligence and security capabilities cannot be turned on and off like a tap. To meet their responsibilities, they must be maintained, and funded in a sustainable way."[11] To some extent, the ISC was becoming involved in advocacy on the agencies' behalf.

Having taken an interest in the agencies' internal procedures, the now Labour-dominated ISC returned to these in the wake of the August 1997 revelations of former MI5 officer David Shayler, soon to be joined by those of former MI6 officer Richard Tomlinson. Frustrated by what he saw as an antiquated approach to management in general and personnel issues in particular, Shayler had gone public when he failed to secure what he felt was a fair hearing of his grievances internally. Among his revelations, Shayler disclosed the names of a few people on whom MI5 kept personal files, extending to the man to whom they were accountable, Home Secretary Jack Straw, and including other Cabinet members, thereby reviving an issue of particular sensitivity on the Labour left. He also alleged that MI6 had been involved in a plot to assassinate Libyan leader Col. Qaddafi. The ISC responded by returning to the question of personnel policies, vetting, and internal security at relative length.[12] However, it refused to meet or take evidence from Shayler and showed no interest in investigating his allegations of an assassination plot.

The Shayler revelations did, however, lead to a renewed interest in the issue of MI5's files. In its 1997–98 report, the ISC confirmed that MI5 held approximately 250,000 hard copy personal files, with an additional 40,000 held on microfiche, and they outlined the process of opening, storing, and classifying these files—the first time this had been done. Concerned at Shayler's ability as an MI5 officer to call up the files of any politician or celebrity that took his fancy, the ISC recommended that access should be restricted to those "with a clear need to see them" and be accompanied by a detailed audit trail indicating who had seen any file, when, and for what purpose.

From the vantage point of the late 1990s, of even greater concern than MI5's historic maintenance of such an extensive number of personal files was the question of the destruction of those files. The ISC was able to bring considerable light to bear on MI5's approach to file retention/destruction. It revealed that until 1970 MI5 had a policy of weeding and destroying files. However, this had affected its ability to pursue a number of espionage cases. Hence, the policy shifted from destruction to microfiching. However, the ISC revealed that in 1992 MI5 "reconsidered its files policy again in the light of the changing nature of the threat with the end of the Cold War and the decline in the threat from subversion." As a result, MI5 began reviewing and destroying personal files on a case-by-case basis, destroying and concealing aspects of its own history in the process. As ISC member Yvette Cooper argued:

> I accept that only the Security Service can make the operational decision whether it still needs to retain a file and continue to use it, but, once the service has decided that it does not need it, there is an historical—not operational—decision to be made. History is not an operational decision. There is absolutely no reason why only the Security Service should be capable of deciding whether something has historical significance for the future. In fact, for the sake of the credibility of history, someone other than the Security Service should make that decision.

> It is controversial stuff. We have all heard the allegations about the monitoring of so-called subversives in the 1970s and 1980s. For all I know, none of it may have happened. On the other hand, all sorts of outrageous things may have happened. The point is that future generations have a right to know what happened and how the organs of the state behaved. They have a right to be able to learn from that and to know that what they are looking at is the entire record. They need to be confident about that. For the sake of credibility, it should not be the Security Service that decides that. Future historians should never be able to say that the service was given a licence to write its own history.[13]

By the time the ISC investigated the issue, 110,000 files had either been destroyed or marked for destruction, the "vast majority" of which related to subversion. The ISC found that "Ultimately, the judgement in respect of the review and destruction of individual files is made solely by the Security Service," and recommended that "some form of independent check should be built into the process, particularly in respect of files relating to subversion."[14]

In sum, the 1997–98 report suggested a more assertive ISC, possibly a consequence of having developed greater self-confidence, possibly a consequence of its changed composition, but most likely a combination of the two. Having initially reassured the Prime Minister and Parliament that its structure was well suited to its task, the ISC had by this point become aware of the fact that it had no investigatory capability of its own, and without this it could not "make authoritative statements on certain issues." Hence, it argued that an investigatory arm would "reinforce the authority of any findings that we make, and be an important element in establishing public confidence in the oversight system."[15]

Two innovations followed from this report: firstly the government began the practice of producing a published response; secondly, it granted an annual parliamentary debate on the reports. In its first Response, the government rejected the ISC's proposal that some form of independent check should be built into the process by which MI5 files were reviewed for destruction. It also asserted that access to files was already restricted and subject to audit arrangements, raising the question of why the ISC, assumed to have access to information on such processes, made the recommendation in the first place. It also seemed to resist the introduction of an investigative arm.

There are two further noteworthy dimensions to this response. First, while the ISC was reporting to the Prime Minister on its oversight of the agencies, in formulating its response, the government was clearly working closely with the intelligence agencies in framing their joint rejection of certain of the ISC's proposals. In other words, the government had established the ISC to oversee the agencies but joined forces with the agencies to reject recommendations arising from this oversight. The response found in favor of the agencies and its continued information monopoly rather than in favor of greater openness and accountability. Second, the timing of the government's response was significant. One of the weaknesses of the ISC structure highlighted in the debates over the Intelligence Services Bill had been that the executive would dictate the timing of

publication. Here, a report that was published after a nineteen-month gap had to wait a further three months for a government response and parliamentary debate. Hence, Parliament was unable to debate the 1997–98 annual report until November 1998.

Parliamentary debate served to highlight concerns about the ISC on the part of its own members and the House of Commons in general. For example, it quickly exposed concerns about the implication for select committees' ability to oversee matters that now fell under the remit of the ISC. In practice, the existence of the ISC could allow the government to justify a refusal to disclose information to select committees—as, indeed, it would on several occasions in the future, most significantly over the highly sensitive question of intelligence and the case for war in Iraq.

Debate also kept the question of the desirability of a move toward select committee status alive. Allan Rogers referred to the ISC's own "strong debates on the possible adoption of a Select Committee style for our proceedings." Fellow ISC member Dale Campbell-Savours did not "believe that oversight is fully credible while the Committee remains a creature of the Executive—and that is what it is. The problem at the moment is that the Committee considers its relationship with the Prime Minister more important to its operation than its relationship with Parliament. I strongly dissent from that view and find the arguments in favour of Select Committee status utterly overwhelming."[16]

One reason why a narrow majority of ISC members came to believe that select committee status was unnecessary was that they saw an alternative route—further evolution of the ISC, and in particular the idea that an investigatory arm should be established. As Yvette Cooper, one of the most articulate advocates of expanded oversight, argued:

> At the moment, information is provided by agency chiefs and by Ministers at their discretion, which raises a difficult point: how can we have proper oversight if the very people whom we are supposed to be overseeing are determining what information we get? That severely jeopardises the Committee's ability to pronounce with authority on important intelligence issues. Credibility demands knowledge and knowledge demands the power to verify—the power to check what is going on. Until now, the ISC has not had that power, and that reduces its credibility in the public mind, as well as in Parliament's mind.
>
> None of that means that I suspect the agencies of any wrongdoing; it means simply that we on the Committee lack the ability to pronounce with confidence that all is well. We cannot come to the House, put our hands on our hearts and say that all is well, because we do not have the power to know.[17]

By the time the ISC produced its 1998–99 report (in August 1999), the government had consented to the appointment of a single investigator, despite some agency unease at the prospect. The investigator, whose terms of reference were dictated by the Prime Minister rather than the ISC, occupied an interesting position,

further inside the "ring of secrecy" than ISC members from whom he could well be obliged to withhold information. Before providing a report on an issue for the ISC, the investigator was required to consult with the agency involved, "so as to allow the Head of the Agency to detemine whether any particular material should be withheld from the Committee."[18]

In its 1998–99 annual report there was further evidence of ISC assertiveness. The Committee argued that it should be granted access to the confidential annexes to the reports of the two commissioners created to investigate warrants in relation to interference with property and complaints referred to them by the tribunals where the tribunal did not uphold a complaint but nevertheless felt that an agency's conduct was unreasonable. On the question of MI5's personal files, its recommendations had contributed toward the creation of a degree of external scrutiny to help ensure that historically valuable documents were not being destroyed. However, the Committee learned that during the period in between the Home Secretary undertaking to review the issue and the announcement that there would be external scrutiny in future rather than suspend file destruction, MI5 destroyed a further 3,000 files.[19] It also continued its campaign to bring greater transparency to the question of the agencies' budgets and expanded its focus on weapons of mass destruction (WMDs), sounding a cautionary note as to the utility of control regimes and treaties and advocating a more proactive approach on the part of MI6 to tracking and frustrating would-be proliferators. In its response, the government refused to make the confidential annexes to the commissioners' reports available to the ISC on the basis that they fell within the category of information defined as "sensitive" in the 1994 Act. It also continued to resist the ISC's attempts to bring greater transparency to the question of agency budgets and rejected the notion that it placed too much faith in control regimes and treaties when it came to countering the spread of WMDs, although its subsquent policy toward Iraq suggested it rapidly lost this faith.

The timing of the report's publication and the government's response was again tardy in the extreme. A report completed in August 1999 was only published in November 1999, the government's response was published at the end of January 2000, and the parliamentary debate finally held in June 2000, almost a year after the report was completed and just two months before the subsequent annual report was presented to the Prime Minister. The delay in publication, response, and scheduling of debate meant that this "annual" debate was held a full twenty months after the previous one.

Although the ISC was established as a self-tasking body, in September 1999 it agreed to the government's request to investigate the policy and procedures employed by the agencies in their handling of information acquired through Soviet defector Vasili Mitrokhin and the events that culminated in the publication of the first volume of his account of Soviet espionage, coauthored with the agencies' favorite academic, Christopher Andrew.[20] This was also interesting in that it was made clear on establishing the ISC that "the past is another country." Now the ISC was being invited to investigate those parts of that country where it

could be helpful to the government. Central to this case were issues of agency accountability to ministers and the degree to which ministers were kept informed about espionage issues. The key case was that of Melita Norwood, code-named HOLA, who the Mitrokhin papers allowed to be identified as a Soviet spy as long ago as 1992 but whom MI5 effectively decided against prosecuting. In 1999, when the first volume of the *Mitrokhin Archive* was about to be published, MI5 asked for an opinion on a possible prosecution, only for the attorney general to advise that a court would be likely to view such a prosecution as an abuse of process, given that no action had been taken when Norwood's identity had first become known. The ISC concluded that

> it was a serious failure of the Security Service not to refer Mrs Norwood's case to the Law Officers in mid 1993. This failure to consult the Law Officers resulted in the decision whether or not to prosecute Mrs Norwood effectively being taken by the Security Service. The Committee is concerned that the Service used public interest reasons to justify taking no further action against Mrs Norwood, when this was for the Law Officers to decide. We also believe that the failure of the Security Services to interview Mrs Norwood at this time prevented her possible prosecution.[21]

In a report highly critical of aspects of MI5's performance, the Committee also said that the Norwood case should have been kept under review between 1993 and 1998 and not allowed to "slip out of sight." That it did represented "a further serious failure." MI5 Director General Sir Stephen Lander would subsequently refer to this ISC report as representing a "public kicking" for the agency.[22]

The government had needed to be seen to launch some kind of investigation into the Mitrokhin/Norwood affair. The ISC was the ideal vehicle, given that original documents would remain within the ring of secrecy and not be made public, as was likely under alternative forms of inquiry. However, the ISC had made clear that to undertake the investigation it needed full access to information, including the normally sacrosanct advice to ministers, a development that caused some concern within MI5. As the ISC reported, "Although there was some delay in reaching agreement about the papers, the request was eventually met in full." This access further emboldened the Committee. Nevertheless, despite working to achieve a high level of mutual trust with the agencies, the Committee was never informed of the Mitrokhin/Norwood issue, even after a decision had been taken to publish the *Mitrokhin Archive*. Hence, although this episode demonstrated that the ISC was not afraid to criticize the agencies, and that it was increasingly self-confident, it also left hanging questions about the degree of accountability it was achieving, thereby affecting public confidence in it.

The 1999–2000 Report continued to provide evidence of assertiveness and the beginning of the emphasis that the ISC would henceforth give to the failure of the Prime Minister to regularly convene the Ministerial Committee on the Intelligence Services (CSI), responsible for approving the National Intelligence Requirements, and which would enable senior ministers to take a collective

strategic view of the challenges and priorities in the fields of security and intelligence. On investigation, the ISC discovered that this body had not met at all since 1995 and that the civil service committee that shadowed it, the Permanent Secretaries' Committee on the Intelligence Services, had met just three times. The ISC was clear on this issue: "We believe that there should be a clear recognition and demonstration of the lines of responsibility and authority for these important Agencies. We recommend that CSI should meet, under your Chairmanship, at least annually to approve the National Intelligence Requirements and endorse or approve the Agencies' budgets."[23] It also returned to the question of access to the confidential annexes to the reports of the commissioners and the government's decision to refuse their request, giving a clear warning that this refusal was compromising the Committee's ability to carry out its oversight function: "It is still important for us to see the classified annexes to be able to establish the corrective action that the Agencies have introduced following the Commissioners' identification of errors and thus fulfil our statutory requirement to oversee the Agencies' administration processes."[24]

Its analysis of the intelligence contribution to the 1999 Kosovo campaign was so heavily redacted as to be without meaning. Elsewhere, it advocated greater intelligence resources be applied to combating drug trafficking, recommended greater resources be committed to combat tobacco smuggling, and expressed concern at the scale of illegal immigration. In its response, published in December 2000, some four months after the report was submitted, the government accepted the ISC recommendation that the CSI should meet annually. However, it maintained its refusal to allow the ISC access to the annexes to the commissioners' reports.

The ISC produced an interim report in March 2001, in anticipation of the calling of a general election, marking the final contributions of a majority of the Committee, including Chairman King. The report once again criticized the government over the failure of the CSI to meet, despite a government commitment that it should do so, leading the ISC to reiterate that it believed that "it is important for the senior cabinet ministers to be properly briefed on the overall performance of the Agencies and we repeat our recommendation that CSI meets at least annually to review this."[25] Elsewhere, it reiterated its disappointment in the government's refusal to publish fuller agency budget figures (in its response the government again declined) and continued to press for the creation of an employment tribunal capable of hearing the grievances of agency staff to prevent the emergence of further Tomlinsons and Shaylers, something over which the government continued to drag its feet. It again asked the government to reconsider its refusal to grant access to the commissioners' confidential annexes, and the government again declined. In sum, the picture that emerged at the end of the Tom King era was of a Committee that had worked hard to establish itself, had evolved its own terms of reference, had gained a significant degree of trust from the agencies, had been critical of both government and agencies on occasion, and had probed government repeatedly in an attempt to secure access to a full range of

information. Yet in the nature of its responses and its handling of the reports, responses, and debates, the government inevitably had the upper hand. Nevertheless, emboldened by its access to material and ability to demonstrate a safe pair of hands over the Mitrokhin affar, the ISC concluded this phase of its development by suggesting a further evolution, in which the past was not necessarily another country. It concluded the interim report by warning:

> One of the characteristics of the intelligence and security field is the frequent, often sensational but unsubstantiated reports that appear in the media. The Committee takes an interest in such matters and seeks to determine which require action by the Committee. A case in point is the allegation of support for a plot to overthrow Colonel Gaddafi. We intended to report to you on this matter but are not yet fully in a position to do so. We believe that the Committee's Report on the Mitrokhin Archive demonstrated our competence in this area, providing an objective view of events with conclusions and recommendations for future work and any necessary changes.[26]

This would represent a significant expansion of the ISC's role, and it remained to be seen whether the significant personnel changes in the wake of the 2001 general election would affect this determination.

THE ISC UNDER ANN TAYLOR, 2001–2005

Following the 2001 general election, the government appointed a new ISC in August comprising five new members and chaired by one of these, Ann Taylor, a former Labour Chief Whip. It produced its first annual report in May 2002, covering the security and intelligence environment in the aftermath of the terrorist attacks of September 11, 2001 (9/11). In it the ISC again pointed to the fact that the CSI had still to meet, although the Prime Minister had convened ad hoc meetings of a similar composition after 9/11. On the question of the 9/11 attacks, a significantly redacted section of the Report showed that, prior to that time, Afghanistan had not been a high priority for the agencies. As the Foreign Secretary, Jack Straw, told the ISC, "the West [had] essentially walked away from Afghanistan, we are trying to get it back."[27] A joint summit of U.S. and U.K. intelligence agencies had spent time discussing Osama bin Laden prior to 9/11, but he remained a "hard target" for the agencies with a specific lack of intelligence on his thinking:

> A JIC assessment in July 2001 suggested that UBL organised attacks were in their final stages of preparation. While US or Israeli interests were the most likely targets, UK interests were at risk, including from collateral damage in attacks on US targets. This lack of intelligence access to a notably hard target meant that the UK and the US did not know who was going to carry out the attacks, how the attacks were going to be mounted or where the attacks were going to take place. Up to that point the West had not foreseen suicide attacks taking place on the USA mainland and certainly not

that the attacks would result in some 3,000 deaths, including the single greatest loss of UK citizens' lives to terrorist attack.[28]

Was this an intelligence failure? The Committee was guardedly ambivalent. The agencies had recognized that there was a "pressing need" to gather intelligence on bin Laden, and ministers had been told that this was in hand; a July 2001 JIC paper had correctly assessed that planning for attacks on Western targets was in the final stages, although it did not present this as a "stark warning" of a threat to the United Kingdom; the conjunction of these facts and Bin Laden's track record "could have warned all concerned that more urgent action was needed to counter this threat." It concluded that with hindsight, "the scale of the threat and the vulnerability of Western states to terrorists with this degree of sophistication and a total disregard for their own lives was not understood."[29] The government's response, drawn up with agency input, defended the agencies' record in relation to the threat from Al Qaeda, declined to make a commitment to follow the ISC's strong and repeated recommendation that the CSI meet at least annually, and continued to refuse to allow the ISC access to the confidential annexes to the commissioners' reports. At this point, the ISC threw in the towel on the question of access to the annexes. If it believed, as it said it did, that access to these was necessary for it to fulfill its mandate, it now appeared to be settling for partial fulfillment.

In October 2002 the ISC was asked by the Foreign Secretary to undertake an inquiry in relation to the adequacy of warnings prior to the Bali bombings of that month, which killed 190 people, including 24 Britons. Its report was critical of the threat assessment produced by MI5. It concluded that MI5 made a "serious misjudgement" and failed to "assess the threat correctly" in not raising the threat level from significant (the third highest level on a six-point scale) to high (the second, behind imminent). At the same time, it reassured Parliament and the public that on the basis of the available intelligence, the attacks could not have been prevented. However, the implication was clear: MI5's threat assessment had been wrong. The ISC also suggested the addition of a further level between significant and high to "allow the threat to be better described for the recipients of the Security Service assessments." As in response to the previous annual report, the government's response included a staunch defense of the agencies and a rejection of the ISC's conclusion that the threat level should have been higher at the time of the bombings. Nevertheless, it also revealed that as a result of a Security Service review rather than ISC recommendations, "threat level definitions have been reworked to give greater definition between levels, to make them more informative to customers and to better support the selection of appropriate protective measures."[30] Similarly, it revealed the establishment of the Joint Terrorism Analysis Centre, an evolution from the multiagency Counter-Terrorist Analysis Centre established after 9/11.

The ISC's 2002–2003 annual report was published in June 2003, in the wake of both the 2003 Iraq war and the controversial case for war presented to the public

by Prime Minister Tony Blair and senior Cabinet members. Again, it took up the fact that the Prime Minister had declined to convene a meeting of the CSI despite the repeated strong recommendations of the Committee, offering its opinion that "CSI Ministers are not sufficiently engaged in the setting of requirements and priorities for secret intelligence, nor do they all see the full capability of intelligence collection."[31] Bizarrely, the government's response was to agree "that CSI has an important function especially in relation to the resourcing and future prioritisation of the Agencies' work, and should meet when appropriate to consider this work."[32] In reality, the Prime Minister had given no indication that he attached any importance whatsoever to either the CSI or the ISC's continual highlighting of its failure to meet. However, on December 18, 2003, some eight years after its previous meeting, the CSI finally met, although it was not to be the beginning of the regular series of meetings that the ISC strongly recommended.

The Committee reported separately, in September 2003, on the question of prewar U.K. intelligence on Iraq's WMDs, which had been fundamental to the Prime Minister's case for war in Iraq. In March 2001, Tom King warned, "We must remember that intelligence can be wasted, ignored—especially if it does not accord with the prejudices and preconceptions of the person on whose desk it falls—used for the wrong purposes or misdirected. The Committee exists to monitor those matters and to try to ensure that mistakes are not made."[33] The corollary of this was that intelligence could be exaggerated. This was the charge leveled at Prime Minister Blair in relation to his case for war with Iraq. This also represented the kind of controversial issue that for some observers would represent a litmus test of the ISC's ability to hold the agencies to account and deal objectively with an issue of great political sensitivity. How would the ISC deal with this?

The ISC sought "to examine whether the available intelligence, which informed the decision to invade Iraq, was adequate and properly assessed and whether it was accurately reflected in Government publications."[34] It did not consider the decision to go to war per se. It reported four months later that based on the intelligence it had seen, there was convincing intelligence that Iraq had active chemical, biological, and nuclear programs and the capability to produce chemical and biological weapons. At the heart of the controversy over prewar intelligence on Iraq was a dossier produced by Downing Street in September 2002 and containing intelligence cleared by JIC Chairman John Scarlett.[35] In its 2002–2003 annual report, the ISC had noted this and said that it "supports the responsible use of intelligence and material collected by the Agencies to inform the public on matters such as these." The question here, then, was how far this represented responsible use of the material, and how far it informed the public as opposed to misled them. However, the ISC did not rise to the challenge, offering no commentary on evidence that the political case was in advance of the intelligence case for war. For example, in a draft of Tony Blair's foreword to the dossier, it was acknowledged that there was no threat of nuclear attack on the United Kingdom, but this had been excluded from the published version. This denied the public available reassurance, removed an opportunity to bring some context to bear, and

served to heighten the sense of threat posed by Iraq. In a tame criticism, the ISC contented itself with observing that "it was unfortunate that this point was removed from the published version of the foreword and not highlighted elsewhere."

The government's response was a further stage in the presentational game that had begun in earnest with the September 2002 dossier itself. It emphasized those aspects of the ISC report that appeared to support its conduct over the production of the dossier and rejected its criticisms. For example, with regard to the charge that the dossier was misleading, its response was that

> the dossier did present a balanced view of Iraq's CBW capability based on the intelligence available. The dossier made clear (paragraph 14, page 16) that the withdrawal of the United Nations Special Commission (UNSCOM) had greatly diminished the ability of the international community to monitor and assess Iraq's continued efforts to reconstitute its programmes. It also noted (paragraph 13, page 16) that UNSCOM was unable to account for significant quantities of agents, precursors and munitions.[36]

But the government cannot have it both ways. Either—as this and the objective record both suggest—the intelligence picture on Iraq was characterized by a significant degree of uncertainty, or, as Blair wrote in his foreword, it was known that Iraq represented a "current and serious threat to the UK national interest." The ISC was dissatisfied with the government's response, as it "emphasised only four key conclusions while either rejecting or failing to address fully many of our other conclusions and recommendations. We regard this as extremely unsatisfactory. . . . Our dissatisfaction was increased by the Government's decision to allow such little time for parliamentary debate" on its Iraq and annual reports.[37] As a result, the government response to the 2003–2004 annual report began a practice of responding to each of the ISC's conclusions individually. However, it did not deal directly with the core question, simply stating, "We regret that the Committee found [the] response unsatisfactory."[38] This did not amount to effective oversight. Key questions had gone unanswered, and the ISC had effectively run out of options in the face of the government's refusal to engage with it. Its investigation had been limited, its findings dismissed by government, and its credibility damaged.

Moreover, it emerged that although the ISC had stated that it had seen all JIC assessments on Iraq produced between August 1990 and September 2002 and the eight produced in the period October 2002 to March 2003, in fact eight had been withheld—five from the former period, three from the latter. Although the Committee was "satisfied that knowledge of them would not have led us to change the conclusions, including those that were critical, in our Report,"[39] earlier access would have allowed it to include further material, and their conclusions would have been more securely rooted in a fuller picture.

Read in the context of the steady spread of democratic oversight of intelligence in the past thirty years, one thing is very striking about ISC reports published before 2005—the complete absence of explicit reference to human

rights. In 2005, however, the ISC reported on an issue at the heart of the global war on terror: the treatment of those detained in Afghanistan, Guantánamo Bay, and Iraq. Paying careful attention to its own boundaries, the ISC investigated any involvement in or witnessing of abuse by intelligence personnel, the adequacy of training as to what to do if it was witnessed, and when ministers were informed of any concerns. Its report rehearsed the relevant conventions on treatment of prisoners, noting that the United States did not regard those detained in Afghanistan as covered by them. The substance of the report was taken up with cases in which intelligence personnel reported their concerns at the treatment of detainees by U.S. personnel; found that these were relatively few (fewer than 15 out of over 2,000 interviews witnessed); criticized the lack of training of staff in convention matters before deployment to Afghanistan, Guantánamo, and Iraq; and noted that when concerns were expressed to U.S. authorities, these were inadequately followed up.

Overall, the report does not provide adequate oversight; certainly the actions of British soldiers lie within the remit of the Defence Select Committee, and the ISC noted that a number were court-martialed, but the Committee did not even explore the issue that soldiers might have prepared detainees for interrogation as U.S. evidence shows. The ISC noted widespread concern about the use of information obtained under torture and briefly noted the pragmatic and principled arguments but did "not attempt to answer these difficult questions." Instead they quoted at length the Foreign Secretary's utilitarian justification for using such information if necessary. Moreover, just as revelations on Iraq subsequent to the ISC investigation left its conclusions there looking thin, so too ongoing revelations about the involvement of U.K. intelligence personnel in the handling and interrogation of detainees have raised questions about the reliability of this investigation.

CONCLUSIONS

In its 1997–98 annual report, the ISC recognized that:

> It is vital that public confidence is maintained in the Agencies. At times of grave national threat, their value is readily accepted. At other times, in the face of a bungled operation or security lapse, public confidence can be very fragile. That is the inevitable consequence of operating within the "ring of secrecy", which prevents a more balanced public view of their activities and their value. The public must therefore be confident that there is adequate independent scrutiny and democratic accountability on their behalf, by people within that "ring of secrecy".[40]

How far has the ISC succeeded in this? In attempting to answer this, other questions need to be considered: What was the government's purpose in creating the ISC? Was it to provide accountability or give the appearance of accountability

and thereby satisfy growing demands for some form of accountability? Fundamentally, the ISC was set up to serve the executive, and that is what it does. Even disagreements between the ISC and executive, or examples of ISC assertion, serve the executive because they confirm the appearance of accountability and thereby dampen demands for more far-reaching accountability, or the introduction of legislative accountability through a select committee of the House of Commons.

Who guards the guardians? This question needs to be adapted slightly to ask: To whom are the oversight committee accountable? Members are accountable to the Prime Minister, and beyond this to themselves collectively and individually. There is no *parliamentary* accountability. This is significant in that the ISC has proved itself unable to be overly critical of executive failures. It can adequately monitor the financial and administrative dimensions of the agencies on behalf of the executive, but not the actions of the executive on behalf of the legislature. Part of the oversight function should be to do precisely this.

Any assessment of the ISC must consider areas of omission as well as commission. For some observers, the real test for the ISC would come when it was faced with a scandal of comparable gravity to those that had been revealed in the years prior to its establishment. Though the question of politicization of intelligence has emerged as an area of central concern in the post-9/11 environment, it is an issue for which the ISC has shown no appetite. Appointed by the executive, reporting to the executive, and holding membership at the pleasure of the executive (in the majority of cases, also the party leader), it has failed to explore the question of executive responsibility.

There are other areas of omission, for example, regarding the Shayler allegations—particularly relating to his allegation that MI6 was involved in a plot to assassinate Col. Qaddafi. Despite the fundamental nature of the allegations, despite some support within the ISC for undertaking an investigation, and despite the fact that Foreign Secretary Robin Cook had been willing to see the ISC investigate the lesser matter of possible Foreign Office connivance in breaking an arms embargo on Sierra Leone, the ISC has failed to address the issue and thereby offer the public the reassurance of which it spoke in its 1997–98 annual report. Issues relating to Northern Ireland have been largely absent from the ISC's published record but, in the light of the Stevens inquiry report, continue to cause concern. Questions that the case of Katharine Gun might have raised about tasking and policy regarding espionage aimed at the UN Secretary General have been avoided.

Despite the advances made by the ISC, particularly in the years up to 2001, as it stands, the scope of intelligence accountability in the United Kingdom lags behind that of other Western democracies. It even lags behind that of the emerging Eastern European democracies, such as Romania and Poland—as the ISC themselves have acknowledged. A significant component of it should be parliamentary debate, a dedicated opportunity for ISC members to speak in the chamber and offer the reassurances that their oversight function is being carried out to their satisfaction and amplifying areas of concern identified in their reports. However,

full parliamentary debate was slow arriving. There was no set debate on the reports until 1998, before the events of 9/11 they were poorly attended, the early debates were held after a significant time had elapsed from the production of the relevant annual report, and when ISC members were critical of the government's response or failure to respond to specific issues, they were effectively ignored.

Oversight of intelligence, whoever carries it out, is inescapably political, and those conducting it must remember that they are engaged in contests of power in which the stakes are high. Shortly after the ISC was established, Peter Gill suggested that a significant indicator of its political will would be "the struggles that take place over access to information. If there are no such battles then we would be justified in concluding that the ISC has failed to challenge central information control."[41] There have been too few of these in the post-9/11 era—the Committee proudly records in the preface to its annual report that it has agreed all government redactions from its annual reports. An oversight committee might be expected to contest at least some of these. This state of affairs suggests a committee too deferential to the executive and too willing to accept deletions. The key area of contest with the executive—over access to the confidential annexes to the commissioners' report—was conceded. To rebuild public and parliamentary trust post-Iraq, the ISC needs to engage in these contests over information.

There are additional limitations or weaknesses that must be considered in any assessment of the ISC. Given the environment in which it must operate, a strong chairman is essential, and in this respect it is worth noting that the elements of role enhancement mentioned in this chapter essentially took place under King's chairmanship. It can be too easily distracted by events, particularly because it is capacity-limited and needs to choose its subjects for inquiry very carefully. In this respect, its decision to dispense with the services of its investigator—after praising his work in successive annual reports—is very disappointing. It was clearly a reaction to his public comments concerning the Blair government's case for war in Iraq. The Committee needs to expand its investigatory and staff base rather than remove it in response to pressure, real or perceived, from agencies or executive. Moreover, there is a very real sense in which post-9/11, the ISC's definition of its role has come to focus more on intelligence management and concern that the agencies are adequately funded at the expense of legislative oversight of the executive branch.

On a more positive note, the ISC was tasked with performing intelligence from scratch, with no more guidance as to how to go about this in practice than that provided by the bare bones of the 1994 Intelligence Services Act. It has put considerable flesh on these in the years since then, expanding its remit in the process. In practice, it has also taken an interest in operational matters, despite these falling outside its remit—for example, in investigating issues relating to the Kosovo campaign, WMD proliferation, Sierra Leone, and the Mitrokhin affair. Moreover, it has introduced significant accountability with regard to the agencies' finances, previously an area of limited transparency even at ministerial level. Indeed, until 1994 there was no external auditing of the agencies' accounts. It is

also undoubtedly the case that the very existence of the ISC has given the agencies cause to reflect on proposed actions in advance of undertaking them. At one time, referred King to "a tendency now within the agencies to ask what the Intelligence and Security Committee would think if they embarked on a certain course of action" and suggested that this "could be used in the future against Ministers who want intelligence in areas that the agencies do not think fall within their remit."[42]

Does the ISC represent a first step on the road to fuller accountability, or the best feasible balance between competing demands? During parliamentary debate on the Intelligence Services Bill, MPs were divided on this point. Yet it seems inevitable that the ISC of 1994 will come to be seen as having represented a first step on the road to accountability. As such, in the wake of the division and distrust engendered by the government's presentation of its case for war in Iraq, the time is ripe for an additional step, so that accountability structures retain the confidence of the public they are designed to reassure. In June 2000 ISC member Dale Campbell-Savours told the House of Commons: "The arguments about whether the ISC is a Select Committee will simply be cast aside by history. The process is inevitable; it will happen."[43] However, the treatment of Dr. David Kelly, who committed suicide after a particularly fierce grilling by the Foreign Affairs Committee, has meant that any agency enthusiasm for such a development has been extinguished for now. Nevertheless, it remains a necessary step for the achievement of the fullest feasible degree of accountability.

NOTES

I thank Peter Gill for his comments on an earlier draft of this chapter.

1. Tony Geraghty, *The Irish War: The Military History of a Domestic Conflict* (London: HarperCollins, 1998), chap. 4.
2. *New Statesman*, December 12, 1986, p. 7.
3. John Willman, "Secret Service Open to Scrutiny," *Financial Times*, November 25, 1993.
4. *Hansard*, February 22, 1994, col. 171.
5. *Hansard*, April 27, 1994, col. 351.
6. *Hansard*, February 22, 1994, col. 240.
7. *Interim Report of the Intelligence and Security Committee* (ISC), Cm 2873, May 1995, para. 8.
8. ISC, *Annual Report 1995*, Cm 3198, March 1996, para. 7.
9. Ibid., para. 37.
10. ISC, *Annual Report 1996*, Cm 3574, para. 6.
11. ISC *Annual Report 1997–98*, Cm 4073, November 1998, foreword.
12. Ibid., paras. 24–38.
13. *Hansard*, November 2, 1998, col. 612.
14. ISC, *Annual Report 1997–98*, para. 50.
15. Ibid., para. 69.
16. *Hansard*, November 2, 1998, cols. 596, 618.

17. Ibid., col. 610.

18. *Government Response to the Intelligence and Security Committee's Annual Report 1998–99*, Cm 4569, January 2000, para. 34.

19. ISC *Annual Report 1998–99*, available at http://www.archive.official-documents.co.uk/document/cm45/4532/4532.htm, November 1999, para. 79.

20. Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West* (London: Allen Lane, 1999). "The SIS regarded Professor Andrew as a safe pair of hands [who] was also security cleared and had signed the Official Secrets Act." ISC, *The Mitrokhin Inquiry Report*, Cm 4764, June 2000, para. 46.

21. Ibid., para. 34.

22. Sir Stephen Lander, "The Oversight of Security and Intelligence," speech at Royal United Services Institute, London, March 15, 2001.

23. ISC, *Annual Report 1999–2000*, Cm 4897, Nov. 2000, para. 19.

24. Ibid., para. 35.

25. ISC, *Interim Report 2000–01*, Cm 5126, March 2001, para. 15.

26. Ibid., para.34.

27. ISC, *Annual Report 2001–02*, Cm 5542, June 2002, para. 54.

28. Ibid., para. 63.

29. Ibid., para. 65.

30. *Government Response to the Intelligence and Security Committee Inquiry into Intelligence, Assessments and Advice Prior to the Terrorist Bombings on Bali 12 October 2002*, Cm 5765, February 2003, para. 10.

31. ISC, *Annual Report 2002–03*, Cm 5837, June 2003, para. 56.

32. *Government Response to the Intelligence and Security Committee's Annual Report 2002–03*, Cm 5838, June 2003, para. 10.

33. *Hansard*, March 29, 2001, col. 1149.

34. ISC, *Iraqi Weapons of Mass Destruction—Intelligence and Assessments*, Cm 5972, September 2003, para. 11.

35. On this, see Mark Phythian, "Hutton and Scott: A Tale of Two Inquiries," *Parliamentary Affairs* 58, no. 1 (January 1995), pp. 124–37; Peter Gill and Mark Phythian, *Intelligence in an Insecure World* (Cambridge: Polity, 2006), esp. chap. 7.

36. *Government Response to ISC Report on Iraqi Weapons of Mass Destruction—Intelligence and Assessments*, Cm 6118, February 2004, para. 13.

37. ISC, *Annual Report 2003–04*, Cm 6240, June 2004, para. 87.

38. *Government's Response to the Intelligence and Security Committee's Annual Report 2003–04*, Cm 6241, July 2004, para. P.

39. ISC, *Annual Report 2003–04*, Cm 6240, June 2004, para. 146.

40. ISC, *Annual Report 1997–98*, foreword.

41. Peter Gill, "Reasserting Control: Recent Changes in the Oversight of the UK Intelligence Community," *Intelligence and National Security* 11, no. 2 (April 1996), p. 328.

42. *Hansard*, March 29, 2001, col. 1149.

43. *Hansard*, June 22, 2000, col. 512.

5

DOCUMENTARY EVIDENCE FOR DIFFERENCES BETWEEN AMERICAN AND BRITISH APPROACHES TO INTELLIGENCE

LAWRENCE J. LAMANNA

THE WAR IN IRAQ, THOUGH TRAGIC, OPENED for scholars and the public a unique window into the world of intelligence: the release of parallel British and American documents related to the prewar intelligence on Iraqi weapons of mass destruction (WMDs). The purpose of this chapter is to exploit this opportunity by comparing these documents to determine what they reveal about differences between British and American approaches to intelligence concepts, structures, methods, purposes, and philosophies. This analysis provides concrete and replicable evidence of differences between the two systems based on directly comparable data. It also provides a convenient and brief description and chronology of the development of these documents.

This study is not, however, an evaluation of the performance or failure of the intelligence apparatus of the United States and the United Kingdom. Neither does it seek to judge whether policy makers and political leaders in either country made proper or improper use of intelligence products. Finally, this chapter is not about Iraq as such.

Among the differences observed in this study are the following:

- When agencies disagree on intelligence findings, the American system allows for the expression of dissent from the majority view, whereas the British system simply excludes the controverted finding.
- American intelligence reports include explicit levels of confidence; British reports do so only vaguely and occasionally.
- British intelligence reports provide greater historical context and take a more narrative form than do American reports.

- The British are more interested in hearing the assessments and analytical opinions of foreign governments and experts than are the Americans. The Americans look to foreigners mostly for collection purposes, not analytical or estimative ones.
- British intelligence agencies and government departments cooperate and collaborate with one another to a high degree, American agencies do not.
- In the American system, the various intelligence agencies come together to produce the most important intelligence reports. In the British system, the intelligence agencies *and* other departments of government come together to produce the most important reports that incorporate intelligence information.
- The American and British political systems (i.e., presidential versus parliamentary) interact with their respective intelligence communities differently, and this may lead to different practices and norms.

METHODOLOGY

The method of the chapter is simple and straightforward. Both sets of documents were read and observations about the systems, concepts, and methods were noted. Then the observations were compared and differences between the two sets were analyzed.

This chapter is deliberately observational: an effort was made to let the documents speak for themselves without bringing theoretical preconceptions to the analysis. In other words, it is not an attempt to find evidence supporting any particular theory of institutions or organization. In this regard, it is a type of case study that Levy refers to as atheoretical or configurative-idiographic: "Idiographic case studies are inductive; they involve a minimum of a priori theoretical preconceptions, and the interpretation emerges from the case itself."[1] The only conscious, working hypothesis is that despite the extremely close cooperation, the shared history, and the "special relationship" between the United States and the United Kingdom intelligence services, there will be some detectable differences in methods, organization, and concepts.

Anyone familiar with intelligence studies will know that there are some generally acknowledged differences between these two national systems. Yet the observation of these differences is frequently personal and impressionistic. The current study is not entirely free from impression either, but the sources of those impressions are publicly available documents. In this respect, therefore, it is concrete and replicable: another researcher could access the same documents and verify or challenge the findings of this study.

BACKGROUND, DEFINITIONS, AND DOCUMENTS

Rarely is there a contemporary glimpse into the workings of the national intelligence apparatus of either the United States or the United Kingdom. Typically, intelligence reports and related documents are released to the public only decades after the events or situations they describe. Memoirs or first-person accounts may be more contemporary, but they are often difficult to verify and are frequently interpretive. Because of the controversies surrounding Iraq, the United States and the United Kingdom both made a remarkable amount of intelligence information available to the public before the war. After the war and because of the subsequent loss of confidence in intelligence capabilities, both nations initiated high-level investigations into their own intelligence apparatus and products. These investigations placed even more information into public view.

Specifically, in fall 2002 the United Kingdom released *Iraq's Weapons of Mass Destruction: The Assessment of the British Government*,[2] and the United States released *Iraq's Weapons of Mass Destruction Programs*.[3] Both documents were written for public consumption, but both were also closely related to one or more classified reports.

By summer 2004, investigations into the quality of the underlying intelligence had been completed in both countries. On July 7, 2004, the U.S. Senate Select Committee on Intelligence (SSCI) released a redacted version of its results, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*.[4] On July14, the Butler Committee in the United Kingdom released *Review of Intelligence on Weapons of Mass Destruction*,[5] otherwise known as the Butler Report (see Volume 4, Appendix G). In addition to these reports, the Central Intelligence Agency (CIA) also released two heavily redacted versions of a classified intelligence report.

There are three other documents that should be mentioned, although they are not included in the current analysis. First, on September 9, 2003, the Intelligence and Security Committee (ISC) of the U.K. Parliament delivered its investigative report, *Iraqi Weapons of Mass Destruction—Intelligence and Assessments*, to the Prime Minister.[6] This report is excluded because it is not directly comparable to any U.S. report due to its production date. The U.S. and British intelligence estimates were finalized within a few weeks of each other in the fall of 2002. Similarly, the Senate report and the Butler Report were both finalized in July 2004. The Butler Report (BR) acknowledges the usefulness of the ISC report, but it also notes that the Butler Committee had two important advantages over the ISC: the further passage of time and "much wider access to the Government's intelligence and policy papers" (BR 2). The timing of an investigation affects the results, and therefore it is important that the timing match to compare national reports.

Second, the British government released a document to journalists at the beginning of February 2003 that contained some information produced by the intelligence services.[7] This document was excluded from the current analysis

because, in addition to information produced by British intelligence, it contained unattributed information from other, nongovernmental sources that made it quite controversial and unusual. On the American side, there is nothing comparable to this document, and its treatment in the British investigative reports is minimal.

Finally, on March 31, 2005, the Presidential Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the Silberman-Robb Commission) released an unclassified version of its report (see Volume 4, Appendix F).[8] Unfortunately, because this investigation concluded almost nine months later than the other two in the analysis, it also suffers from the mismatched time problem. Furthermore, its findings and characterizations are not independent of the others. The Silberman-Robb Commission acknowledged in its own report that the Butler Report was "an important resource" and the Senate report was "particularly valuable."[9] The report of the Silberman-Robb Commission is an important contribution to understanding what went wrong with U.S. intelligence, but because it was influenced by the Butler Report, it does not represent a purely national perspective.

At this point, a brief explanation of top-level intelligence reports is in order. Both the United States and the United Kingdom have intelligence services that produce information, analysis, and reports for policy makers at the highest levels. In the United States, the epitome of these products is a National Intelligence Estimate (NIE). "NIEs are long-term intelligence products that attempt to estimate (not predict) the likely direction an issue will take in the future. Ideally, NIEs should be anticipatory, focusing on issues that are likely to be important in the near future and for which there is sufficient time to arrive at a community-wide judgment."[10] An NIE may outline several possible directions that events may take, providing a judgment or estimate of the likelihood of each. NIEs are highly classified documents that are normally not released to the public until decades have passed after their production.

Each NIE is prepared under the supervision of a National Intelligence Officer (NIO), of which there are currently twelve.[11] Some NIOs have a geographic responsibility, such as the NIO for Africa, and others have topical responsibilities, such as the NIO for Economics and Global Issues. Together with a chairman and staff, the NIOs make up the National Intelligence Council (NIC). NIEs are systematically and formally circulated and discussed among the sixteen agencies that make up the U.S. intelligence community and finally approved by the Director of Central Intelligence (DCI).[12]

The British product that corresponds to an NIE is an Assessment.[13] Assessments are produced by the Joint Intelligence Committee (JIC) Assessments Staff.[14] The JIC is a Cabinet committee composed of the heads of the three British intelligence and security agencies; the chief of Defence Intelligence; senior policy advisors from the Foreign Office, the Ministry of Defence, the Home Office, the Treasury, and the Department of Trade and Industry; and representatives of other departments as necessary. These civil service policy advisors and department heads report to and assist government ministers in the formulation and execution

of policy. The committee meets weekly and provides a key link between policy makers and intelligence services; it both reports intelligence to policy makers and communicates intelligence requirements to the agencies.

Figure 5.1 presents a chronology of the documents examined in this chapter and also notes the abbreviations that will be used to cite them.

THE U.S. ESTIMATE AND WHITE PAPER

The CIA released three related documents that are part of this study. The first of these is the public white paper, *Iraq's Weapons of Mass Destruction Programs*, released on October 4, 2002. Work on this document began in May, but in some ways the drafts were overtaken by events and the final document became a reflection of the classified NIE that was produced on October 1 (SEN 287).

The white paper is twenty-five pages long; contains color pictures, maps, and charts; and is clearly intended to show the danger that was Iraq. It describes nuclear, chemical, biological, ballistic missile, and unmanned aerial vehicle (UAV) programs. It also provides some history of UN resolutions and UN inspection operations related to Iraq. On the one hand, some statements and assertions are plainly speculative and the authors indicate higher or lower levels of confidence for some of their assertions. On the other hand, the document presents no dissenting opinions.

The document is structured in the following way:

1. Key Judgments
2. Discussion—Iraq's Weapons of Mass Destruction Programs
   a. Nuclear Weapons Program
   b. Chemical Warfare Program
   c. Biological Warfare Program
   d. Ballistic Missile Program
   e. Unmanned Aerial Vehicle Program and Other Aircraft
   f. Procurement in Support of WMD Programs

The next relevant U.S. document is the *Key Judgments* text.[15] This document was released by the CIA on July 18, 2003, and contains eight pages photocopied from the original, classified October 1 NIE. Specifically, these are pages 5 through 9, pages 24 and 25, and an amalgamation of pages 74 and 84.[16] Large sections of several pages are masked. The first five pages are the key judgments section of the NIE. These pages are similar (but not identical) to the key judgments section of the white paper.

One of the most important contrasts to the white paper is that the *Key Judgments* text reveals some dissension from the prevailing judgments. At the end of the first paragraph of page one of *Key Judgments*, the reader is directed to a box at the end of the "key judgments" section (KJ 4) which explains the dissent of

Figure 5-1. Chronology of Events and Key to Documents

2002	May 8	Request made in the United States for white paper on Iraq's WMD programs
	September 3	British government requests public dossier on Iraq's WMD programs
	September 9	British assessment most closely associated with the British public dossier is produced
		First request (from Sen. Durbin) for an NIE on Iraq's WMD programs
	September 12	DCI orders the production of a NIE on Iraqi WMDs
	September 24	U.K. government releases *Iraq's Weapons of Mass Destruction: The Assessment of the British Government*, an unclassified dossier based on classified assessments (DR)
	October 1	CIA produces NIE 2002-16HC on *Iraq's Continuing Program for Weapons of Mass Destruction* (NIE)
	October 4	CIA releases *Iraq's Weapons of Mass Destruction Programs*, an unclassified white paper related to the NIE (WP)
2003	February 1–2	British Coalition Information Centre shares *Iraq—Its Infrastructure of Concealment, Deception and Intimidation* with journalists
	March 19	U.S. and U.K. invasion of Iraq begins
	June 20	SSCI announces intention to begin formal review of intelligence on Iraqi WMDs
	July 18	CIA releases *Key Judgments* from NIE 2002-16HC (KJ)
	September 9	Intelligence and Security Committee delivers *Iraqi Weapons of Mass Destruction—Intelligence and Assessments* to the Prime Minister
2004	February 3	British government announces Butler Committee inquiry into September 24, 2002, assessment on Iraqi WMDs
	February 6	President George W. Bush issues Executive Order 13328 creating the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Silberman-Robb Commission, SR)
	February 12	SSCI announces expansion of its investigation
	June 1	CIA releases redacted version of NIE 2002-16HC (NIE)
	July 7	SSCI releases redacted version of *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq* (SEN)
	July 14	Butler Committee releases *Review of Intelligence on Weapons of Mass Destruction* (BR)
2005	March 31	Silberman-Robb Committee finishes classified and unclassified versions of its *Report to the President of the United States* (SR)

the State Department's Bureau of Intelligence and Research (INR). In this text the INR notes that although it does believe that Saddam Hussein wants to acquire nuclear weapons, it does not believe that the current intelligence makes a compelling case that he is "currently pursuing what INR would consider to be an integrated and comprehensive approach to acquire nuclear weapons" (KJ 4–5).

The INR statement cites the judgment of experts at the Department of Energy who found that a key piece of evidence against Iraq—the aluminum tubes acquired from abroad—were poorly suited for a nuclear program.[17] For this reason and because of the "atypical lack of attention to operational security" on the part of the Iraqis, the INR expresses its dissent from the majority view on the aluminum tubes (KJ 5). INR also states that it finds "highly dubious" the claim that Iraq was seeking to obtain uranium from Africa (KJ 8). Last, within the key judgments section, the text states that the "Director, Intelligence, Surveillance, and Reconnaissance, U.S. Air Force, does not agree that Iraq is developing UAVs *primarily* intended to be delivery platforms for chemical and biological warfare (CBW) agents" (KJ 3, emphasis added). The Air Force believed that the primary role of Iraq's UAVs was for reconnaissance. Although it is not reproduced in *Key Judgments*, further elaboration of this dissent regarding UAVs is included in a footnote at a later point in the NIE. At least part of that footnote has been revealed in the Senate report (SEN 225), in spite of the fact that it is masked in the declassified NIE.

Another notable difference between *Key Judgments* and the white paper is that *Key Judgments* includes caveats such as "we judge" before some assertions (see also SEN 286–89). These phrases have the effect of reminding the reader that a judgment is being expressed, not a statement of indisputable fact. The white paper does not include these caveats and therefore gives the impression that there is no serious doubt about its assertions.[18]

On June 1, 2004, the CIA released yet another version of what can now be identified as NIE 2002-16HC.[19] This final version consists of the original cover, a two-page errata sheet that was referred to in the earlier releases, and the ninety-three pages of the document body. One page of the errata sheet and all but twelve pages of the body of the document are completely masked. Of the pages with text on them, the only new pages are the cover, a title page, and two pages at the end which list the agencies involved in preparing the NIE and all of the NIC officers. In other words, the release is mostly blank pages. The rest of the visible material was available in the *Key Judgments* document. Page numbering is now visible, though, and that reveals the relative positions of the previously released pages.

The NIE states that it was "prepared under the auspices of Robert D. Walpole, National Intelligence Officer for Strategic and Nuclear Programs"; with assistance from the NIOs for Near East and South Asia, Science and Technology, and Conventional Military Issues (NIE title page). This NIE was requested by members of the SSCI, who wanted more information available as they considered

authorizing military action against Iraq (SEN 9). The NIE was mainly authored by former CIA Deputy Director John McLaughlin.[20]

THE BRITISH DOSSIER

The British dossier was released by the government on September 24, 2002. It is fifty-one pages long and includes maps and photos. The dossier was commissioned on September 3 and largely based on three classified JIC assessments dated March 15, August 21, and September 9, all of 2002. The September 9 assessment, which focused on various "attack scenarios," was the most influential of the three (BR 79–80, 83).

From the beginning the dossier was conceived of as a document for public consumption to help explain government concerns regarding Iraq. According to the foreword by Prime Minister Tony Blair, the document as published was "based, in large part, on the work of the Joint Intelligence Committee" (DR 3). Subsequent reports indicate that the dossier was in fact authored by the JIC and that the executive summary was authored by the chairman of the JIC, John Scarlett.[21]

In many respects the content is similar to the American documents, which is not surprising given the high level of intelligence and military cooperation between the two countries. Also, both countries were relying heavily on information from the UN inspection teams for a period of time, so they were getting essentially the same information.

The structure of the dossier is as follows:

1. Forward by Prime Minister Tony Blair
2. Executive Summary
3. Iraq's Chemical, Biological, Nuclear, and Ballistic Missile Programs
   a. The Role of Intelligence
   b. Iraq's Programs 1971–1998
   c. The Current Position 1998–2002
4. History of UN Weapons Inspections
5. Iraq under Saddam Hussein

DIFFERENCES BETWEEN THE ESTIMATES

There are a number of differences between the British and the American documents. The British dossier has more historical information and is written in a more narrative style than the American white paper or NIE. It provides more detail about individuals such as Iraqi scientists, government officials, and relatives of Saddam Hussein. In addition to describing Iraq's weapons programs, it lays out a history of Hussein's rule and his many human rights abuses. It

also asserts a connection between the threat or use of force and consequent Iraqi cooperation with inspections and the UN Security Council. The dossier gives more detail about what the UN Special Commission (UNSCOM) and the International Atomic Energy Agency (IAEA) teams found and it attributes information to them when appropriate. The dossier more frequently reports the official position of the Iraqi government with respect to each issue, including more mention of the transgressions to which Iraq has admitted.

The U.S. NIE is more explicit than the British document about stating levels of confidence for the various specific estimates. Again, it should be noted that these statements are not explicit in the public 2002 version, but they are there in the unclassified portions of the NIE. Although the British dossier does use words and phrases like "probably" and "may have" to express some uncertainty, there are very few negative statements, such as "we do not know." One of the few statements of this kind is in reference to the aluminum tube question. The dossier states that "there is no definitive intelligence that [the specialized aluminum] is destined for a nuclear programme" (DR 26). Another striking characteristic of the British dossier is the number of statements that in one way or another argue along the lines of "what else could it mean but . . . ?" This could simply be the result of excluding uncertain things from the report.

It is commonly understood that the British assessment system produces reports without dissent.[22] This belief is supported by these documents. In the American documents there are explicit dissents from the main conclusions. Most notably this is seen when reporting on Iraq's nuclear program and capabilities. There is nothing like these alternative views in the British dossier. Of course, the actual, classified British assessments are not available for public inspection, but they were available to the Butler Committee and the Butler Report makes no mention of dissenting opinions.

There is also a difference in preparation time. The NIO for the Near East and South Asia began work on the U.S. white paper in May 2002, although there may have been some adjustment in purpose and focus after a meeting between George Bush and Tony Blair at Camp David in early September 2002 (SEN 55, 287; BR 72). This meeting seems to be the point of origin for the British dossier. On the one hand, the American white paper was worked on for about five months, and the British dossier was produced in fifteen days. On the other hand, the British dossier was largely based on an assessment that had just been completed, whereas the American NIE was hurried through in twenty days and the white paper altered to match it.

There is one last observation about the differences between the British and American estimates worth noting. The British dossier includes at least one case of classic British understatement. Regarding the 1990 invasion of Kuwait it states, "When [Saddam Hussein's] threats and blandishments failed, Iraq invaded Kuwait on 2 August 1990. He believed that occupying Kuwait could prove profitable" (DR 47).

THE REPORT OF THE U.S. SENATE

On June 20, 2003, Senator Pat Roberts and Senator John D. Rockefeller IV, the chairman and vice chairman of the SSCI, respectively, announced that the Committee would investigate the following items:

- the quantity and quality of U.S. intelligence on Iraqi weapons of mass destruction programs, ties to terrorist groups, Saddam Hussein's threat to stability and security in the region, and his repression of his own people;
- the objectivity, reasonableness, independence, and accuracy of the judgments reached by the intelligence community;
- whether those judgments were properly disseminated to policy makers in the executive branch and Congress;
- whether any influence was brought to bear on anyone to shape their analysis to support policy objectives; and
- other issues mutually identified in the course of the Committee's review (SEN 1).

On February 12, 2004, the Committee agreed to add to those terms of reference the following items. Those that are listed as phase one are addressed in the July 7, 2004, report (see Volume 2, Appendix H). Those listed as phase two are to be addressed in a future report.

- the collection of intelligence on Iraq from the end of the Gulf War to the commencement of Operation Iraqi Freedom (phase 1);
- whether public statements, reports, and testimony regarding Iraq by U.S. government officials made between the Gulf War period and the commencement of Operation Iraqi Freedom were substantiated by intelligence information (phase 2);
- the postwar findings about Iraq's WMDs and weapons programs and links to terrorism and how they compare with prewar assessments (phase 2);
- prewar intelligence assessments about postwar Iraq (phase 2);
- any intelligence activities relating to Iraq conducted by the Policy Conterterrorism Evaluation Group and the Office of Special Plans within the Office of the Under Secretary of Defense Policy (phase 1 and 2); and
- the use by the intelligence community of information provided by the Iraqi National Congress (phase 1 and 2) (SEN 2).

Committee staff members had already begun reviewing the intelligence on Iraq several months before the committee announced a formal investigation. The committee staff began with 15,000 pages of material from the intelligence community and subsequently requested and received over 30,000 pages more. The committee was denied access to the relevant *President's Daily Briefs* (*PDB*s). The PDB is a daily report provided to the President of the United States by the Director of Central Intelligence (DCI). Without access to the PDB, the committee could

not evaluate the dissemination of intelligence judgments to policy makers (SEN 2–3).

The Committee staff interviewed more than 200 individuals, almost all of whom were officials or employees of the federal government or military services. The staff did interview "nuclear experts with the International Atomic Energy Agency" and former UN inspectors, but it is not clear whether or not these individuals were U.S. citizens. With these individuals as possible exceptions, it seems that the inquiry was conducted entirely within the U.S. government and did not involve information from other governments or non-Americans, except as might exist in the original intelligence products.

The bulk of the work was done by the staff, with the Committee itself holding occasional hearings and giving direction. Part of the method of review was to attempt to ignore and disregard current information on postwar Iraq until an analysis of the prewar information had been complete. The goal was to "replicate the analytical environment [intelligence community] analysts experienced prior to the war" (SEN 4). It is hard to imagine such an attempt being successful.

The report is 511 pages long, all of it text. Although there are quite a few pages with significant portions blacked out, most of the pages are largely in the clear.

The structure of the report is as follows:

1. Introduction
2. Niger
3. Intelligence Community Analysis of Iraq's Nuclear Program
4. Intelligence Community Analysis of Iraq's Biological Weapons Program
5. Intelligence Community Analysis of Iraq's Chemical Weapons Program
6. Intelligence Community Analysis of Iraq's Delivery Systems
7. Iraq WMD Intelligence in Sec. Powell's UN Speech
8. IC Collection Activities Against Iraq's WMD
9. Pressure on IC Analysts Regarding Iraq's WMD Capabilities
10. White Paper on Iraq's WMD
11. Rapid Production of the October 2002 NIE
12. Iraq's Links to Terrorism
13. IC Collection Activities Against Iraq's Links to Terrorism
14. Pressure on IC Analysts Regarding Iraq's Links to Terrorism
15. Powell Speech—Terrorism Portion
16. Iraq's Threat to Regional Stability and Security
17. Saddam's Human Rights Record
18. The IC's Sharing of Intel on Iraqi Suspect WMD Sites with UN Inspectors
19. Appendices, Additional views of particular committee members

The report begins with a description of the training process for CIA intelligence analysts, to put the rest of the discussion into a helpful context for the reader. Particular mention is made of the need to question assumptions and work as a group in which individuals will challenge one another's conclusions.

Of course, the great bulk of the report is about the content and details of the Iraq intelligence and is not especially revealing of American and British intelligence differences. Nevertheless, there are some interesting points for comparison and some points that are simply interesting.

The Senate report reveals that an agency dissenting to some aspect of an NIE can apparently chose how to present its own dissent. In the October 2002 NIE, the INR initially was going to explain its position in footnotes but later "it decided to convey its alternative views in text boxes, rather than object to every point throughout the NIE. INR prepared two separate text boxes, one for the key judgments section and a two-page box for the body of the nuclear section" (SEN 53). Unfortunately, after additional changes to the overall structure of the document, part of INR's dissent on Iraqi efforts to acquire uranium was inadvertently placed in the section dealing with attempts to acquire aluminum tubes, instead of the section dealing with uranium acquisition (SEN 53–54).

The report also reveals that the Department of Energy included at least one extensive text box outlining its dissenting view on the aluminum tubes issue (SEN 95). This text, however, remains classified.

The Senate report notes that managers do not necessarily review the raw intelligence on which an assessment is based. This is especially true if the analyst is more senior and experienced. Editing will be performed, but not necessarily substantial review, and therefore "it is entirely possible that one analyst's views may be presented to high-level officials including the President of the United States without having been reviewed by other analysts with the same depth of knowledge" (SEN 8). This should not be possible for an NIE, however, because it is by definition a collaborative report.

Nevertheless, in the case of the October 2002 NIE on Iraq, the time frame was short and some steps were skipped. The NIE was first requested on September 9, 2002, by Senator Richard Durbin (D-IL), a member of SSCI. This request was followed the next day by another from Senator Bob Graham (D-FL), the chairman of SSCI at that time. By the morning of September 12, the DCI had directed the NIO for Strategy and Nuclear Programs to take the lead in producing an NIE on Iraq's WMD capabilities. Three other NIOs were also directed to work on the NIE. It was understood that the production cycle would need to be fast to meet the congressional need for information prior to voting on legislation. On September 23 the lead NIO circulated a draft to the agencies of the intelligence community, and then two days later held an all-day meeting with community analysts to coordinate changes. A second draft was circulated on September 26. Contrary to standard procedure, the NIO "did not submit the draft for peer review or to a panel of outside experts" (SEN 13).[23] On October 1, the NIE was approved by a meeting of the National Foreign Intelligence Board (NFIB) and printed the same day. The NFIB is chiefly composed of the heads of the various intelligence agencies and is chaired by the DCI. The NFIB normally approves NIEs, but it is not clear how often the board meets in person or whether it met in person to approve this NIE. In all, the process took twenty days. In

interviews conducted for the Senate report, NIOs told the staff that they would prefer to have three months to produce an NIE (SEN 11).

Regarding interagency work and collaboration, the report states this: "Depending on the product, the analysis may be coordinated with other [intelligence community] members, but in many instances, each agency produces its own finished products which are subject to review and editing by its own internal management" (SEN 7). The report also identifies agency rivalry and compartmentalization within a single agency (especially the CIA) as problems (SEN 26–29, 268–71). Presumably, some of this is motivated by source protection and some of it by ordinary bureaucratic turf protection. The report finds that this lack of openness between agencies or even within an agency can interfere with what the British call "validation." Validation includes the process of vetting a source, which is a key to giving appropriate weight to the information coming from the source. If an analyst is denied information about a source, it then becomes more difficult to weight that source appropriately.

The dual role of the DCI—head of the CIA and head of the whole intelligence community—is identified as a source of failure. The report asserts that in fact the DCI functions mostly as head of the CIA and that collaboration and sharing of information between agencies suffers as a result. One illustration of this can be seen in the following. The DCI told the committee staff that he does not even expect to learn of dissenting opinions until an issue comes up in the production of an NIE. Prior to that point, "debate about significant national security issues may go on at the analytical level for months, or years, without the DCI or senior policymakers being informed of any opinions other than those of CIA analysts" (SEN 29, 139). Furthermore, the CIA and the DCI are regularly put in the position of presenting information to the President and other policy makers that is supposed to represent the thinking of the whole intelligence community. This means that they must often present dissenting opinions (when they are aware of them) that they do not share, which calls into question the effectiveness of the presentation.

The creation of the Director of National Intelligence (DNI) in December 2004 has, of course, changed this dynamic. The DCI still heads the CIA, but the DNI now has responsibility for overall management of the U.S. intelligence community and for the presentation of intelligence estimates to the President. This should go a long way toward eliminating the overrepresentation of CIA views in intelligence viewed by the President.

The report states that U.S. intelligence "relies too heavily on foreign government services and third party reporting, thereby increasing the potential for manipulation of U.S. policy by foreign interests" (SEN 34). The report is referring to intelligence collection and does not address whether the United States could actually benefit from foreign analysis and assessment help.

Finally, the committee found no evidence that administration officials attempted to coerce or otherwise influence analysts to change their judgments (SEN 272–84).

THE BUTLER REPORT

The Butler Committee was created on February 3, 2004, and consisted of five members led by Lord Butler. The terms of reference for the committee were:

- to investigate the intelligence coverage available in respect of WMD programs in countries of concern and on the global trade in WMDs, taking into account what is now known about these programs; as part of this work;
- to investigate the accuracy of intelligence on Iraqi WMDs up to March 2003, and examine any discrepancies between the intelligence gathered, evaluated, and used by the government before the conflict, and between that intelligence and what has been discovered by the Iraq survey group since the end of the conflict;
- to make recommendations to the Prime Minister for the future on the gathering, evaluation, and use of intelligence on WMDs in the light of the difficulties of operating in countries of concern (BR 1).

Also, the Prime Minister asked that the Committee produce its report before the summer recess. The Committee was charged to follow a method of inquiry modeled on the Franks Committee that investigated the Falklands War.[24] The Committee was to submit its final conclusions "in a form for publication, along with any classified recommendations and material" (BR 1). The main product was meant to be public, with additional classified materials available to the government.

The five Committee members held a total of thirty-six meetings. The Committee interviewed officials within the British government and intelligence services, including the Prime Minister. The Committee also traveled to the United States to meet with senior officials, members of Congress, and the staffs of the CIA and the Defense Intelligence Agency. The Committee traveled to Baghdad to meet with some military leaders and Charles Duelfer, the special advisor to the DCI on Iraq's WMDs. Duelfer's work was important to the Butler Committee because his findings would be the most complete standard against which the Committee could measure the prewar assessments. Unfortunately, the work of the Iraq Survey Group, which Duelfer headed, was not completed before the Butler Committee's deadline. Nevertheless, they were able to obtain preliminary information from Duelfer that allowed them to make some judgments.

The Butler Committee approach was to examine the assessments produced by the JIC and then examine the antecedent and underlying intelligence—both what was accepted and what was rejected. They would then consider "whether it appears to have been properly evaluated" (BR 3). Another method used in the Butler Report was to compare assessments and data that have been made public through some other process, such as a report by the United Nations or the IAEA. Once information entered the public domain in some other way, the Committee had no concerns about drawing attention to it for the purpose of presenting its

findings. This allowed it to make its points without revealing more classified material.

The report was issued on July 14, 2004, and consists of 196 pages of text, with nothing blacked out. One of the annexes at the end includes portions of three classified assessments.

The structure of the report is as follows.

1. Introduction
2. Nature and Use of Intelligence
3. Countries of Concern Other than Iraq and Global Trade
4. Terrorism
5. Counter-Proliferation Machinery
6. Iraq
7. Iraq: Specific Issues
8. Conclusions on Broader Issues
9. Summary of Conclusions
10. Annexes

In the introduction, the report thanks the intelligence agencies for their cooperation and work and declares that the Committee is "relatively confident" that they have been provided all of the relevant data. They also note that the British intelligence community coordinated its efforts so that the Committee received a single stream of papers and data, not a separate one from each agency. This would seem to indicate a high level of bureaucratic trust, cooperation, and ability to work together. Consistent with this, the report attributes success in exposing the nuclear proliferation network established by A. Q. Khan, a Pakistani physicist, to "strong integration in the U.K. between all agencies." It notes that a decision was made to share even the most sensitive information at the working level. There was also a "high degree of co-operation between agencies and policy-makers in departments" (BR 20). This integration was further enhanced by the creation of the Joint Terrorism Analysis Centre in June 2003 (BR 36). The center brings together staff from eleven different government agencies and departments.

Like the Senate report, the Butler Report takes some time to describe the intelligence process. The model that the Butler Report lays out consists of four steps: collection, validation, analysis, and assessment.[25] The report explains collection as mainly made up of signals intelligence (SIGINT), information from human sources (HUMINT), and imagery information (IMINT). It describes the other three steps in this way: "Validation should remove information which is unreliable (including reporting which has been deliberately inserted to mislead). Analysis should assemble fragmentary intelligence into coherent meaningful accounts. Assessment should put intelligence into a sensible real-world context and identify how it can affect policy-making" (BR 14).

Validation has as much to do with the faithful transmission of the information through the intelligence collection agency as it does with the quality of the source.

In the British system, the Ministry of Defence receives the largest quantity of intelligence and the analysis stage is carried out there by the Defence Intelligence Staff (DIS). The report states that "analysis can be conducted only by people expert in the subject matter" (BR 10). So, though validation looks at both the source and the chain of communication, analysis looks at the factual substance of the information, evaluates it, and tries to make sense of it. The report states that "assessment may be conducted separately from analysis or as an almost parallel process in the mind of the analyst" (BR 10). Furthermore, "in the U.K., assessment is usually explicitly described as 'all-source' " (BR 11). The goal with assessment is to be as objective as possible, unaffected by motives and pressures that might distort judgment (BR 12). The report notes that in the United Kingdom, "central intelligence assessment is the responsibility of the Assessments Staff." This staff is made up of approximately thirty senior and middle-ranking officials on assignment from other departments, along with secretarial and administrative support. The staff is housed within the Cabinet Office.

The JIC brings together the intelligence agencies, the DIS, and important policy departments. The Chief of the Assessments Staff is also a member of the JIC. The JIC meets weekly. In addition to regular attendees, government departments send officials as matters warrant. Representatives from the intelligence communities of Australia, Canada, and the United States also attend on occasion. The chairman of the JIC has at times also been the prime minister's Foreign Policy Adviser. "The JIC thus brings together in regular meetings the most senior people responsible for intelligence collection, for intelligence assessment and for the use of intelligence in the main departments for which it is collected" (BR 13).

In addition to conventional and direct national interests, JIC assessments also support inspection, monitoring, and verification regimes in other parts of the world to prevent the proliferation of nuclear, chemical, and biological weapons (BR 38). This indicates a vision for intelligence that goes beyond immediate state security interests to longer range interests.

As noted earlier, JIC assessments do not contain minority reports or dissents. "When the intelligence is unclear or otherwise inadequate and the JIC at the end of its debate is still uncertain, it may report alternative interpretations of the facts before it such as they are; but in such cases all the membership agrees that the interpretations they are proposing are viable alternatives. The JIC does not . . . characterise such alternatives as championed by individual members who disagree with colleagues' points of view" (BR 13). The JIC has also made the assertion that when intelligence is ambiguous it should not be artificially simplified. The Butler Report includes extensive quotations from JIC assessments.

The report identifies several examples of JIC assessments where the "JIC made clear that much of the assessment was based on its own judgment" (BR 75). By this the authors seem to mean that the assessment was based not on new information but on speculation and logical extrapolation from previously known facts. This type of reporting seems particularly problematic in a context where the providers of intelligence and the consumers of intelligence are working together

and are sometimes one and the same. In the absence of hard data, policy preferences are likely to be indistinguishable from assessments. Despite this, the committee found no evidence that senior policy officials on the JIC improperly influenced assessments in a preferred-policy direction (BR 110).

However, there was concern about politicization resulting from publicity. The report notes that the dossier broke new ground in three ways:

- The JIC had never previously produced a public document.
- No government case for any international action had previously been made to the British public through explicitly drawing on a JIC publication.
- The authority of the British intelligence community, and the JIC in particular, had never been used in such a public way (BR 76).

Material from the JIC had been used in public before, but it had never been attributed. To the Butler Committee, this is a major change with worrisome consequences (BR 114). The concern is that bringing intelligence into the public arena will tempt everyone to use it as a political tool and eventually as a partisan political tool. Americans would tend to frame this as an issue of transparency and see attribution as a positive step. To them, the greater danger of politicization arises from the strength of the relationship between intelligence producers and policy makers.

The Butler Committee saw a need to slightly modify the position and choice of the chairman of the JIC. Currently, this person may be outranked by the heads of the intelligence agencies that sit at the JIC. The Butler Committee concludes that the person chosen as chair should be very senior and in the latter stage of his or her career in the government. In sum, the chair should be beyond influence and have more clout in both the intelligence community and the policy community (BR 144).

The committee also suggests expanding and developing both the JIC Assessments Staff and the HUMINT collection capacity of the agencies. There is insufficient collection in some areas. At the same time there is insufficient capacity to analyze the information that is collected.

As mentioned earlier, the public dossier was heavily influenced by the September 9 JIC assessment. According to the Butler Committee, "The most significant difference was the omission of the warnings included in JIC assessments about the limited intelligence base on which some aspects of those assessments were being made" (BR 80).

The committee also suggests that the JIC enhance the ability of assessments to convey levels of confidence, and it draws attention to the U.S. practice of doing this explicitly, along with notes of dissent (BR 145).

In a couple of places the Butler Report mentions compartmentalization as problem, but only very briefly (BR 111, 139). This problem was much more prominent in the Senate report on the American system. In fact, the Butler Report and the British dossier seem relatively comfortable discussing secrets that have already been revealed through some other source.

Finally, the Butler Report notes some management weaknesses with human sources in the Secret Intelligence Service (BR 102–9). These were indirectly the result of staff cuts and could easily be fixed by reversing the cuts and reinstituting previous practices. These do not seem to indicate any major differences in British and American approaches.

DIFFERENCES BETWEEN THE INVESTIGATIVE REPORTS

First, there are some obvious differences. The Butler Report, which is final, consists of 12 pages of front matter and 196 pages of report. The Senate report is two-and-a-half times longer with 9 pages of front matter and 511 pages of report, and it is only the first of two phases of investigation and reporting. The British report was produced by a Committee of five members: two current members of Parliament (one from the government, the other from the opposition), two former high-ranking civil servants, and one former high-ranking military officer (former chief of defense staff). The Committee had a staff of seven plus additional interview transcribers. The American report was nominally produced by a congressional committee of seventeen members (plus the Senate Majority and Minority Leaders, who are ex officio members of SSCI), no doubt with a much larger staff that did a greater share of the actual work. This disparity in size may be attributable to the disparity between the two nations in resources and international responsibilities, but one suspects that it is at least partly a reflection of relative efficiency.

The British focused their investigation on ensuring validity from the beginning of the evidence chain to the JIC. Because the JIC represents both the producers of intelligence and the consumers of final assessments, it is not subject to some of the assessment problems that occur in the American system. For instance, the Senate report describes the problem of layering (SEN 22–23, 212). This happens when new assessments are based on old assessments, which are based on even older assessments. The key danger with this practice is that the caveats and uncertainties of the earlier assessments may be left out in later ones that almost treat the earlier ones as sources. This causes the reader of the current assessment to think that it rests on a stronger foundation than it does. Previous estimates become conventional wisdom rather than true estimates with particular levels of confidence. When the new estimate reaches the policy maker, he or she is not aware of its true contingency. Although it may still occur, this problem is less likely to occur in a system where those incorporating the intelligence into final policy advice are included in the assessment process. They are more likely to know the history and the genesis of the assessments to which they are contributing and agreeing.

Closely related to the layering problem is that of failing to properly identify assumptions. Both reports are concerned with the possibility that worst-case

calculations are mistaken for the prevailing wisdom of what is most likely to develop (BR 46).

Countering the possible benefit the British derive from the JIC system is the danger of politicization of intelligence that most American observers would anticipate from a close proximity of analysis/assessment and policy making.[26] The concern is that known policy preferences will cause analysis to be skewed in favor of supporting those preferences. As one American scholar/practitioner has succinctly put it, "Only by maintaining their [analysts'] distance from policy can they hope to produce intelligence that is objective."[27] The CIA has an Ombudsman for Politicization specifically to deal with the problem of pressure from management or policy makers, and the Senate report includes a chapter on the issue of improper political pressure (SEN 357–65). The Butler Report is not greatly concerned with the relatively close working relationship of intelligence producers and intelligence consumers in the JIC. It notes that "the JIC has always been very conscious" of the need to be objective (BR 16).

Surprisingly, the Senate report does not include a list of recommended changes. This may have fallen outside of their self-determined mandate for political reasons. The Republicans in control of the Committee may have wanted to leave the President's hands free or they simply may not have reached a bipartisan agreement on what changes to recommend. Another explanation is that they did not believe large changes were politically feasible, given the history of the U.S. intelligence community and the great number of individuals and institutions that have a stake in the current arrangements. For instance, all of the various congressional committees and subcommittees that have some control over the intelligence community would likely resist restructuring efforts that would lessen their control. Other departments of government (for example, the military services and the Justice Department) would also fight changes if they meant losing their share of intelligence activities and information sources. Given its public failures and the legislation to reorganize the intelligence community that was passed after these reports were written, it is unlikely that the committee felt that no structural changes were needed.

The Butler Committee did provide explicit recommendations in their report, and this may be a result of the fact that their mandate came from the executive in a parliamentary system where the executive is, of course, also the legislative leader. In such a system, the interest and ability in making changes is much more likely to be consistent.

Both the Senate report and the Butler report identify information sharing within their respective governments and intelligence communities as a problem, but in the British system it is a rather minor anomaly, whereas in the United States it is systemic and normal to refrain from sharing information with other agencies and departments. This is also seen directly in the investigative work of the committees. In the United Kingdom, the investigators eventually had access to all of the information they requested. In fact, the intelligence agencies were able to work together to provide requested information through one source,

regardless of its origin. In the United States, the investigators had to negotiate with each agency and the White House. Despite the fact that during the Senate investigation the Senate and SSCI were controlled by the President's political party, they were not granted access to everything that they wanted, most notably the *President's Daily Briefs*.[28] The presidentially appointed Silberman-Robb Commission, though, was granted full access to these documents, which supports the idea that institutional rivalry between the executive and legislative branches in the U.S. system accounts for some differences between intelligence information availability and use in the American and British systems. It is also noteworthy that the American NIE and the first major postinvasion investigation of intelligence were both initiated by American legislators, not by the executive branch. At the least, American intelligence agencies exist in a more complex setting of political institutions than their British counterparts.

Another difference between the two approaches is that the United States suffers from a lack of alternate perspectives. Although the U.S. intelligence community has especially strong relationships and interactions—liaison—with intelligence agencies in the United Kingdom, Canada, Australia, and New Zealand, it is telling that no officials from these countries were interviewed or participated in the investigation leading to the Senate report, even though they are surely involved with and pay close attention to what happens with U.S. intelligence. Indeed, as mentioned, the Senate report views reliance on intelligence collection by foreign governments as a potential source of manipulation. The Butler Committee did not limit its interviews to British government employees or British nationals, but interviewed individuals from a variety of nations, including U.S. government officials.

LIMITATIONS

Before drawing final conclusions, the limitations of this study should be spelled out. First, despite the unusual amount of material released, there are still gaps in the documentary evidence. On the British side, although portions of the actual assessments produced by the government have been made public (BR Annex B 163–76), the percentage of the full assessments these represent is unknown. Also, the Butler Commission delivered some additional classified findings to the government that are not included in their public report. On the American side, most of the text of NIE 2002-16HC is still classified and there are masked-out lines scattered throughout the Senate report. Material that is not available to be read cannot be evaluated. If the unavailable material is selected in some manner that is systematically related to the nation of origin, then the conclusions of the current analysis are biased. Further, even if the still classified material does not skew the analysis, it may include some additional national differences that will not be detected by this study. Nevertheless, it is possible that a great deal of what is still classified would not change the current analysis. For

instance, the revelation of protected sources might reveal something about divergent methods, but it is more likely to produce only a list of names.

Second, this chapter looks at only one set of documents for a single time and a single situation that is exceptional in a number of ways. Therefore, there is a question as to whether the evidence reviewed here represents British and American approaches generally. This is a problem of validity—does this data really represent the phenomenon of interest? The data here do provide evidence for the conclusions drawn, but not conclusive evidence. Adding more cases of corresponding British and American documentation would strengthen the conclusions.

Third, there is the question of whether the two investigations and reports are strictly comparable. The American investigation was carried out by the large staff of a legislative committee, the British investigation by a much smaller committee dominated by civil servants. If the Silberman-Robb Committee had formed earlier and finished in the summer of 2004, then it would have more directly corresponded to the Butler Committee. However, as noted, the Silberman-Robb Committee was influenced by both the Senate report and the Butler Report and therefore does not represent a firsthand or exclusively American look at the situation.

As stated at the beginning, this chapter attempts to avoid preconceptions and let the documents speak for themselves. It is, of course, impossible to set aside all preconceptions. The documents examined herein are consistent with some commonly understood differences between American and British intelligence structures, procedures, and attitudes, but they also highlight a few unexamined differences. Even for the former, this chapter provides accessible documented evidence that is sometimes lacking in the literature on intelligence.

CONCLUSIONS

This study has documented a number of significant differences between American and British approaches to intelligence. One of the most noteworthy is the relative ease with which information is shared within the British government. The Butler Committee noted only minor problems along these lines, whereas compartmentalization and information hoarding are major problems in the American system. Without this liberality, the assessments-producing Joint Intelligence Committee would not be possible. The JIC is another important distinguishing structure. In it, the whole government (and sometimes even representatives of foreign governments) is brought together to make assessments, not just the intelligence-producing agencies. This contributes to another distinguishing feature of British intelligence practice, namely, providing greater context for understanding problematic situations. British reports provide more of what anthropologist Clifford Geertz called "thick description," or the detail necessary to understand the meanings and motives of behaviors.[29] This detail might be

historical or cultural or even detail about individuals other than the immediate target of interest—detail that reveals not just functional interactions but also the identities and relationships that shape those interactions.

Another important difference made more salient through the documents in this comparison is the way intelligence information is transmitted to the political executive. During the period when these documents were produced, the formal process in the United States was for the DCI to present intelligence produced by the intelligence community to the President. This created a bias toward the views of the CIA over the views of other agencies, and it also created a competition for the President's ear as other agencies tried to find pathways that bypassed the DCI. In the United Kingdom, the JIC system and the generally cooperative attitudes again seem to avoid this problem. All of the intelligence services are represented on the JIC, which meets weekly, and information presented there is taken by the various department heads back to their departments and their political overseers. The Prime Minister also receives his or her information from the JIC. Therefore, individual intelligence services each have the same opportunity to communicate their efforts to the whole government and do not need to compete with one another for access to the leadership of the government.

Furthermore, the British JIC system forces the leaders of different parts of the intelligence community to sit down together on a weekly basis and reconcile their views. This more frequent personal interaction undoubtedly contributes to their willingness to share information with one another, too. The U.S. NFIB structure is similarly collegial on paper, but does not frequently convene in person and serves mainly as a routing list for reports or conference calls. It also lacks the regular interaction with top policy advisors and nonintelligence department heads as a group.

A final major difference comes from the distributed nature of political power in the American system. Because of the separation of the legislative and executive branches of government, intelligence agencies in the United States face a more complicated environment and a different set of pressures than their counterparts in the United Kingdom. As noted, the legislative branch in the American system initiated both the NIE and the postinvasion investigation; the latter despite the lack of partisan division between Congress and the President at the time. In this environment, intelligence agencies can be subjected to conflicting pressures and can also choose to appeal to either of two (or more) masters. In the British parliamentary system, intelligence producers are far less likely to experience these conflicting pressures because the legislative leadership automatically holds the executive power, too. Though there is a parliamentary Intelligence and Security Committee in the United Kingdom, its role is limited and it does not effectively balance against the government the way that the congressional committees balance against the executive branch in the U.S. system.[30] This is evident in the fact of the ISC's restricted access to government documents, its small role in the Butler Report, and its inability to report to Parliament or the public without the prime minister's approval. For the same reasons, the access of opposition

or minority political parties to intelligence information and influence is also much less in the British system. One implication of this system is that there is no institutional counterweight to check the executive use or misuse of the intelligence services other than the judiciary, which is not likely to get involved unless there is a domestic abuse of power or some other incident that inflames the public.

Besides these major differences between the two systems, there are also some less sweeping but still important differences. Most significant among these are the American practices of including of notes of dissent and communicating explicit levels of confidence in intelligence estimates. Among other things, the Butler Report recommended that the British JIC assessments staff consider adopting these practices.

In conclusion, the current study is only a basic, observational contribution to intelligence studies. It can be built on in several ways. First, documents from additional nations related to the Iraq WMD problem should be examined. Second, comparable documentation describing other problems (not the Iraq case) should be sought out and examined. Both of these steps would expand the number of cases available and may result in a typology of intelligence systems. Third, theoretical explanations for differences or types found should be explored and tested. Why do the British provide more context in their reports? Why can the British departments share information and the Americans cannot? Some researchers are already engaged in efforts to explain the perceived difference in intelligence—policy maker distance using cultural variables.[31] Additional explanatory power might be found in the broader institutional environment or the historical choices of previous governments. Both the rational choice approach and the less individualistic historical institutionalism approach to explaining norms and patterns of behavior would probably be illuminating.[32] Fourth, the implications of different intelligence systems can be explored, assessing their advantages and disadvantages and thus providing useful information for governments and policy makers. With these steps, further comparative analysis can be applied to the field of intelligence studies to reveal important aspects of intelligence systems that go undetected in the more common, single-country studies. This chapter is a modest contribution to that effort.

NOTES

An earlier version of this chapter was presented at the 2006 International Studies Association conference in San Diego, CA, under the title "A Comparison of the United States and the United Kingdom Inquiries into Intelligence Failure: Mining the Iraq Case."

1. Jack S. Levy, "Qualitative Methods in International Relations," in Frank P. Harvey and Michael Brecher, eds., *Evaluating Methodolgy in International Studies*, Millennial Reflections on International Studies (Ann Arbor: University of Michigan Press, 2002), p. 135.

2. Joint Intelligence Committee, *Iraq's Weapons of Mass Destruction: The Assessment of the British Government* (London: Stationery Office of the United Kingdom, 2002), available at http://www.pm.gov.uk/files/pdf/iraqdossier.pdf (accessed October 13, 2004).

3. CIA, *Iraq's Weapons of Mass Destruction Programs* (2002) available at http://www.cia.gov/cia/reports/iraq_wmd/Iraq_Oct_2002.pdf (accessed September 17, 2004).

4. Senate Select Committee on Intelligence, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq* (Washington: Government Printing Office, 2004), available at http://www.gpoaccess.gov/serialset/creports/pdf/s108-301/s108-301.zip (accessed September 17, 2004). This report represents the first part of a two-phase investigation. However, there is serious doubt as to whether the full second phase will be carried out, although some aspects were published by the Committee in 2006.

5. Lord Butler, *Review of Intelligence on Weapons of Mass Destruction* (London: Stationery Office of the United Kingdom, July 14, 2004), available at http://www.official-documents.co.uk/document/deps/hc/hc898/898.pdf (accessed October 13, 2004).

6. Intelligence and Security Committee, *Iraqi Weapons of Mass Destruction—Intelligence and Assessments* (London: Stationery Office, September 11, 2003), available at http://www.cabinetoffice.gov.uk/publications/reports/isc/iwmdia.pdf (accessed September 14, 2005).

7. Coalition Information Centre, *Iraq—Its Infrastructure of Concealment, Deception and Intimidation*, (January 2003), available at http://www.pm.gov.uk/files/pdf/Iraq.pdf (accessed September 14, 2005).

8. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington: Government Printing Office, 2005).

9. Ibid., p. 46.

10. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 2nd ed. (Washington, DC: CQ Press, 2003), p. 49.

11. This discussion of the U.S. intelligence community and its products is based on the system in place at the time the Iraq documents were produced. Some features of this system changed with the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (December 17, 2004). In particular, the creation of the Director of National Intelligence changed the structure and some of the top-level interactions of the intelligence community. This will be discussed further later in this chapter.

12. Lowenthal, *Intelligence*, pp. 102–3. Now, however, the director of National Intelligence has replaced the DCI in this role.

13. Michael Herman, "Assessment Machinery: British and American Models," in David A. Charters, A. Stuart Farson, and Glenn P. Hastedt, eds., *Intelligence Analysis and Assessment*, Studies in Intelligence (London: Frank Cass, 1996).

14. Ibid.; Joint Intelligence Committee, *Iraq's Weapons of Mass Destruction*; Lowenthal, *Intelligence*, p. 236; Jeffrey T. Richelson, *Foreign Intelligence Organizations* (Cambridge, MA: Ballinger, 1988), p. 37.

15. CIA, *Key Judgments (from October 2002 NIE)* (Washington: National Security Archive, 2003), available at http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB129/nie_judgments.pdf (accessed September 20, 2004).

16. Because none of the pages in *Key Judgments* display page numbers, references to pages in this document will follow an ordinal sequence beginning with the first page as page 1.

17. The Department of Energy, however, did not dissent on the issue of whether Iraq had begun to reconstitute its nuclear weapons program.

18. For another useful comparison of the October 2002 white paper with the *Key Judgments* document, see Parliamentary Joint Committee on ASIO ASIS and DSD, *Intelligence on Iraq's Weapons of Mass Destruction* (Commonwealth of Australia, 2003), available at http://www.aph.gov.au/house/committee/pjcaad/WMD/report/fullreport.pdf (accessed November 26, 2004).

19. CIA, *Iraq's Continuing Programs for Weapons of Mass Destruction: NIE 2002-16hc* (Washington: National Security Archive, 2004), available at http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB129/nie.pdf (accessed August 14, 2004).

20. Michael Hirsh, Michael Isikoff, and Mark Hosenball, "Secret Agent Man," *Newsweek*, July 5, 2004.

21. Butler; Michael Herman, "Intelligence's Future: Learning from the Past," *Journal of Intelligence History* 3, no. 2 (2003), p. 3.

22. Percy Cradock, *Know Your Enemy: How the Joint Intelligence Committee Saw the World* (London: John Murray, 2002), pp. 295–96; Herman, "Assessment Machinery," pp. 19–20; Michael Herman, *Intelligence Services in the Information Age: Theory and Practice*, Studies in Intelligence (London: Frank Cass, 2001), pp. 133–34; Loch K. Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (New Haven, CT: Yale University Press, 1996), pp. 128–29.

23. "Outside" in this context appears to mean outside of the group of analysts who prepared it in the first place, not outside of the intelligence community.

24. Lord Butler, *Opening Statement by the Chairman, 14 July 2004* (Butler Committee, 2004), available at http://www.butlerreview.org.uk/news/launchstatement.pdf (accessed December 1, 2004); Butler, *Review*.

25. The report also alludes to requirement setting for collection, but does not treat this formally and perhaps does not consider itself to be evaluating this part of the process.

26. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949); H. Bradford Westerfield, "Inside Ivory Bunkers: CIA Analysts Resist Managers' 'Pandering'—Part I," *International Journal of Intelligence and Counterintelligence* 9, no. 4 (1996–97); but for an empirical challenge to the conventional view, see Stephen Marrin, "Does Proximity Between Intelligence Producers and Consumers Matter? The Case of Iraqi WMD Intelligence," paper presented at the *International Studies Association Conference* (Honolulu: International Studies Association, 2005).

27. Lowenthal, *Intelligence*, p. 142.

28. A daily summary of intelligence produced for the president at that time by the DCI.

29. Clifford Geertz, *The Interpretation of Cultures: Selected Essays* (New York: Basic Books, 1973).

30. The ISC consists of nine members appointed by the prime minister in consultation with the leaders of the two main opposition parties. The members come from both houses of Parliament and are not limited to the governing party. The committee is within the "ring of secrecy" of the Official Secrets Act and reports directly to the prime minister.

31. Philip H. J. Davies, "Intelligence Culture and Intelligence Failure in Britain and the United States," *Cambridge Review of International Affairs* 17, no. 3 (2004); Stephen

Marrin, "Why Does Distance Between Intelligence and Decisionmaking Vary? The Impact of Decisionmaking Culture on Intelligence Analysis," working draft, University of Virginia, 2005. See also Michael A. Turner, "A Distinctive U.S. Intelligence Identity," *International Journal of Intelligence and CounterIntelligence* 17, no. 1 (2004).

32. Peter A. Hall and Rosemary C. R. Taylor, "Political Science and the Three New Institutionalisms," *Political Studies* 44, no. 4 (1996); Lawrence J. Lamanna, "Explaining Differences in British and American Intelligence Norms," working draft, University of Georgia, 2005; Paul Pierson, *Politics in Time: History, Institutions, and Social Analysis* (Princeton, NJ: Princeton University Press, 2004); Kathleen Thelen, "Historical Institutionalism in Comparative Politics," *Annual Review of Political Science* 2, no. 1 (1999).

6

MORE PERFECT OVERSIGHT

Intelligence Oversight and Reform

CYNTHIA M. NOLAN

Of all our recommendations, strengthening congressional oversight may be among the most difficult and important. So long as oversight is governed by current congressional rules and resolutions, we believe the American people will not get the security they want and need. The United States needs a strong, stable, and capable congressional committee structure to give America's national intelligence agencies oversight, support, and leadership.[1]

IN 2004, THE NATIONAL COMMISSION ON TERRORIST Attacks Upon the United States (the 9/11 Commission) revealed its research into the events, intelligence, and decision making leading up to the terrorist attacks of September 11, 2001. Among many other recommendations and criticisms, the Commission members concluded that the congressional oversight of intelligence had been insufficient. They argued that the congressional oversight committees—the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI)—required complete reform. According to the Commission members, only a comprehensive overhaul would accomplish clear accountability for the intelligence agencies.[2]

These recommendations imply that stronger, unified, clearer, more efficient oversight would improve the capabilities of the intelligence agencies, their joint relations, their products, and—consequently—foreign policy decision making. According to the members, more comprehensive, far-reaching, actionable, unified, and—most important—accountable intelligence will help prevent future terrorist acts. Though not specifically mentioned by the Commission, its recommendations were based on the conclusion that intelligence oversight is so unique as to require a unique kind of oversight.

With this research, I ask whether this unspoken assumption is correct. Is intelligence oversight so peculiar that it requires exceptional methods? Likewise, I ask whether those who conduct intelligence oversight believe it is unique and therefore believe it requires exceptional methods or whether the overseers believe traditional methods are sufficient.

Examining this question will require a few steps. First, I review the oversight literature to determine the conduct of congressional oversight. Second, I ascertain whether intelligence oversight is conducted differently from the oversight of other bureaucratic offices. Finally, the chapter examines the opinions of congressional insiders; interviews of current and former representatives and senators should shed some light on the extent to which oversight of the intelligence agencies is unique.

CONCEPTUALIZING CONGRESSIONAL OVERSIGHT

Legislative oversight—the review of executive activities by Congress—can take any one of a few forms. Morris Ogul identified a latent and manifest dichotomy of congressional oversight. In his characterization, members of Congress perform oversight indirectly through their many legislative duties, as well as directly through hearings, reporting requirements, and investigations. In his view, much of what is actually congressional oversight has not been called oversight.[3] He concluded that although latent oversight is not well measured, it is most common.

Joel Aberbach distinguished between advocacy and adversarial approaches to oversight. Legislators may seek to protect bureaucratic offices with which they have become very friendly or perhaps criticize these executive-level administrators for some reasons related to political gain, personal preferences, or their home districts. He further asserted that oversight units are more likely to be neutral.[4] He concluded that advocacy oversight, overall, is more often found in the congressional committees.

McCubbins and Schwartz observed centralized and decentralized oversight activities as the most important dividing line between two types of congressional oversight: police patrol style and fire alarm style. They argued that legislators have chosen fire alarm style, a less expensive, decentralized oversight to review the executive branch activities. On the one hand, the centralized oversight (police patrol style) that most researchers expect to find retains most investigative powers within the congressional committee. On the other hand, decentralized oversight empowers outside observers with the ability to initiate necessary "alarms" triggering oversight responsibilities.[5] They observed that decentralized oversight is most likely in Congress.

Ogul and Rockman also observed an active and reactive dichotomy in the academic treatments of congressional oversight. In these characterizations, they argued that McCubbins and Schwartz's treatment of congressional oversight observed active versus reactive activities as well as centralized and decentralized

oversight. They modified the police patrol oversight, calling it decentralized and active. In select committees, they asserted that oversight is most likely to be centralized and reactive.[6] They observed that in general, reactive oversight is more likely to be found in congressional oversight.

Ogul and Rockman identified one other dichotomy in the academic treatments of congressional oversight: anticipatory and post hoc oversight. They argued that subtle and anticipatory oversight most certainly occurs, but it is difficult to measure. What may be termed unintended reactions influence bureaucratic officers to change their own actions in anticipation of some form of oversight by Congress in this anticipatory oversight.[7] However, they argued that post hoc oversight is the most likely congressional oversight activity.

DEFINITIONS

Legislative oversight is defined herein as the legislation, hearings, investigations, and activities of Congress that review, study, and report on executive branch agencies and offices.

For my purposes, traditional methods of oversight are defined as the most common ones employed in Congress, as determined by outside researchers. Such observers most often describe legislative oversight as latent, advocacy-oriented, decentralized, reactive, post hoc activities.[8] These common attributes therefore describe the most utilized tools and methods of congressional oversight. By contrast, exceptional methods of oversight are those less commonly identified by outside observers. Such methods might be described as manifest, critical, centralized, and anticipatory.[9]

This research begins by listing and describing the most important factors in determining the character of oversight. This step also includes investigation of these factors in relation to the intelligence agencies with a reference to the oversight of other bureaucratic agencies. Using these comparisons, one can determine whether intelligence oversight in its current state is unique. Using interviews with representatives and senators, I then explore how unique intelligence oversight should be. Finally, the chapter examines reform recommendations related to intelligence oversight and ask whether these reforms are necessary.

DETERMINING OVERSIGHT

As already noted, congressional oversight is traditionally considered latent, friendly, decentralized, reactive, and post hoc. Expectations of what oversight should accomplish have infused the opinions and descriptions of how oversight is conducted. Early researchers on this subject found that congressional oversight of the bureaucracy seldom measured up to these ideals.[10] Later research asserted that the expectations of these researchers had been flawed. For instance, McCubbins

and Schwartz argued that the decision is rational to follow fire alarm oversight by building and empowering outside alarms to alert Congress to oversight dangers. Consequently, they found that legislators prefer this type of oversight. Aberbach studied similar concerns in oversight and found that legislators have actually followed a great deal of police patrol oversight because of changes in the congressional context.[11] Thus it is safe to conclude that legislative control of the bureaucracy is some combination of police patrol and fire alarm oversight.

McCubbins and Schwartz emphasize that although Congress will use a variety of methods to oversee the government, they prefer fire alarm oversight because it is most cost-effective. Aberbach agreed that there are many elements of oversight in the legislative arsenal, but nonetheless reached contrary conclusions. Specifically, he decided that the 1970s era of political activism encouraged much more active oversight, and thus more police patrol oversight, than had been prevalent before. The post–Cold War environment likely has encouraged equally active oversight in all areas of government control.

In the area of foreign and defense policy, Christopher Deering asked whether Congress prefers police patrol or fire alarm oversight. Deering first addressed the extent to which these areas of the bureaucracy are unique. He determined that these areas are not so unique as to render the police and fire fighter metaphors inapplicable. He argued that in the House, the National Security and International Relations Committees preferred police patrol oversight during the 104th Congress. The Senate Armed Services and Foreign Relations Committees likewise preferred police patrol oversight during the 104th Congress.[12]

Deering concluded that legislative oversight of foreign and defense policy does not differ significantly from oversight of other bureaucratic offices. In the post–Cold War period, Congress is as willing to participate in defense and foreign policy as it is in other areas of the federal government.[13] Similarly, Aberbach argued in 1990 that the congressional context—relations with the President, resources for the committees and staff, as well as changes in the home districts—changed so dramatically that formal congressional oversight in all areas had increased, making legislators more likely to step publicly into the defense and foreign policy arena.[14]

A few distinct factors stand out in determining this character, quality, and quantity of legislative oversight and how unique or traditional it might be. I now apply them to intelligence oversight.

INFORMATION FLOWS

Lupia and McCubbins examined the decisions of a legislature to delegate policy-making authority to government bureaucrats, as well as the consequences of those decisions. Generally, legislators realize that bureaucrats possess greater expertise than members of Congress. The primary means by which they overcome this deficiency is through oversight. The question for these researchers was

as follows: Under what conditions do legislators' efforts at oversight actually achieve their desired outcomes? The main obstacle to legislators gaining their desired policy choices is information.[15]

The quality of any oversight effort relies to some degree on the quality of information the legislators receive. In some areas of government, information flow is easier, more accessible, and much more likely than in others. One can imagine that consumer products, or medical policy decisions and the information surrounding them, is more accessible than defense or intelligence decisions simply because the information is publicly available. For instance, far more of the reports and documents produced by the intelligence agencies are likely to be classified than is the case with respect to the Consumer Products Safety Commission or the surgeon general, although to be sure, the latter offices do not publish every document they produce and Freedom of Information Act requests to these agencies are common.[16]

If the intelligence agencies classify a greater number of documents than other government agencies and offices, this fact would be a significant barrier to legislative oversight, making intelligence oversight unique. To be sure, the intelligence agencies share a great deal of information with Congress—more every year.[17] This classified information may be viewed by legislators on the intelligence oversight committees—the HPSCI and SSCI—in specialized security storage areas only.[18]

However, one can identify other areas of government oversight that require equally secure handling instructions for legislators of government documents, i.e. social security and consumer credit information, individual medical information, weapons specifications, details of defense assignments, FBI files, or perhaps even sensitive information regarding aircraft or other transportation protocols. Moreover, many critics have accused the current administration of President George W. Bush of over-classifying information since the terrorist attacks of September 11, 2001. Indeed, in 2004, twice as many documents—from the entire government—were classified as in 2001.[19]

Increasing classification (both in volume and breadth) of government reveals that the secrecy that previously set the intelligence agencies apart is spreading to other areas of congressional oversight. Moreover, in response to congressional demands, intelligence agencies share more information with legislators. The barriers to information flow within the system of intelligence oversight seemed obvious at first glance, but closer inspection suggests secrecy may not differ as much as previously assumed.

COMMITTEE HISTORY

The HPSCI and SSCI have just passed their thirtieth anniversaries. Established to respond to egregious abuses by the Central Intelligence Agency (CIA) and other intelligence elements in the government, these committees represented a distinct departure from the prior approach to intelligence oversight. That approach had been distant, marginal, and often silent. The establishment of the

HPSCI and SSCI improved intelligence oversight, and the Committees embraced oversight as their primary objectives.

Thus two historical strains of oversight tendencies influenced the history of the Committees. Institutional oversight is supportive of the intelligence agencies, even unquestioning in its advocacy of this government bureaucracy. Investigative oversight questions the intelligence agencies, exposes potential difficulties, criticizes problems, and punishes mistakes and abuses.[20]

According to Seymour Scher's research on congressional oversight, House and Senate committees tend to resist change without significant outside stimuli.[21] Standard operating procedures along with the time pressures to accomplish current legislative business encourage committees to continue their typical patterns. One standard pattern of intelligence oversight was inquisitive because its inception occurred in such difficult circumstances. However, a strong historical strain of advocacy also influences the intelligence committees. A mix of investigative and institutional oversight results. Aberbach argued that committees almost always operate in a non-neutral environment.[22] The intelligence committees are no exception. A mix of advocacy and criticism is probably found in most congressional committees, making the intelligence oversight committees not especially unique.

SUBJECT MATTER/EXPERTISE

Congressional relationships with bureaucratic agencies are rooted in a trade-off between accountability and expertise. By their very nature, bureaucracies possess more expertise than Congress. A member of Congress could certainly obtain considerable expertise with a significant time commitment, but such a decision would preclude learning in other areas of policy necessary to his or her career. As a result, legislators delegate policy-making authority to bureaucratic agencies while retaining some degree of accountability to Congress. That control manifests in the form of oversight, budgetary controls, statutory instructions, initial procedures and structures, and congressional reviews.[23]

According to Ogul, more technical and complex subjects discourage the likelihood of oversight. Only a few members of Congress are likely to become experts in difficult, labyrinthine subjects.[24] The intelligence agencies are one such example. These agencies have acquired their own language, often as a result of secrecy. Although HUMINT may be easy to understand, SIGINT and IMINT are highly technical subjects requiring significant study.[25] Thus intelligence oversight does stand out as unique (although the labyrinthine language and technical details of the Defense Department are probably equally challenging).

Ogul further asserted that if a subject is concentrated in one administrative agency, it is more likely to be overseen than issues that are spread out over more than one bureaucracy.[26] In this context, the intelligence agencies seem to present a rather difficult situation for Congress. On one hand, there are sixteen separate agencies and offices with intelligence duties. On the other hand, the CIA is easily

the most visible of these. Thus the CIA often receives the most concentrated attention among intelligence watchers. Congress made its oversight of these agencies even more difficult by spreading its oversight responsibility out over at least four committees when the HPSCI and SSCI were created. Some responsibilities for military oversight were retained by the Armed Services Committees, for instance.[27]

The visibility of the subject matter is also important. Subjects related to one's constituents, personal values, career aspirations, or reelection campaign will in all likelihood attract more congressional attention, according to Ogul.[28] Because of the required secrecy that surrounds intelligence matters, it is not an especially visible subject. However, when some public scandal erupts, the subject becomes highly visible. According to Ogul's criteria, intelligence again seems to both repel and attract oversight.

TRANSPARENCY

Relatedly, Charles Shipan rests his analysis of congressional oversight on transparency that exists where citizens can see how policies are made. The more transparent a subject, the more accountable the bureaucratic agency will be. Certain congressional tools will increase transparency, such as detailed statutes telling bureaucratic agencies exactly what to do; public debates, speeches, reports, and votes; open budget process; and congressional riders that specify individual projects favored by a particular member of Congress. Certain other congressional tools will decrease transparency, such as structures and procedures that establish broad parameters for policy guidelines that are not visible to the public, congressional reviews that follow agency decisions made out of the public view, and general reactive oversight legislation.[29]

Intelligence oversight is quite clearly not very transparent. Consequently, Shipan concludes, Congress will be less involved in the policy making of the intelligence agencies. According to Shipan's categories, intelligence oversight would follow a traditional oversight pattern. Nonetheless, oversight of other bureaucratic agencies is much more open and much more accountable.

INTEREST GROUPS

Transparent bureaucratic agencies are more likely to encourage outside interest groups that will aid congressional oversight. In McCubbins and Schwartz's parlance, outside interest groups can pull metaphorical fire alarms to alert Congress to possible problems in a government office. One can imagine that health subjects, education, or housing issues promote outside observers to form coalitions that lobby Congress much more often than intelligence issues. There are few if any intelligence-related interest groups. Thus intelligence oversight—

unlike most oversight subjects—operates without the benefit of additional viewpoints, informal watchdogs, or a strong sense of public opinion. Congress operates without interested groups agitating for additional information. This absence gives fewer incentives for legislators to demand more information and involvement and more incentives for intelligence agencies to give less information and involvement to Congress. Again, the intelligence agencies seem to both attract and repel congressional scrutiny.

UNCERTAINTY AND CONFLICT

When Congress decides to delegate policy-making authority to bureaucratic agencies, it must assess the level of uncertainty with which it is comfortable. These original decisions regarding the level of delegation influence the future of the relations between the bureaucratic agency and Congress. A high level of uncertainty at the start of a policy-making relationship increases the need for oversight at a later date.[30]

In other words, if legislators start with a low level of information, they will need to make up for that deficiency with traditional oversight methods. The intelligence agencies began as separate bureaucratic offices generally in the post–World War II period. The CIA, for instance, was founded in 1947. The National Security Agency (NSA) was started in 1952. At that time, Congress delegated a great deal of policy-making authority to the agencies. Very little information was shared with Congress beyond budgetary needs.[31] Loch K. Johnson calls this the "era of trust." It ended in 1974, when Congress became enmeshed in a long and detailed investigation of domestic spying by the CIA in direct violation of that agency's original 1947 foundation.[32]

Congress did not assert its general responsibility for oversight in a positive way until the 1946 Legislative Reorganization Act. The act for the first time made all congressional committees responsible for "legislative oversight."[33] This newly introduced term did not hand a new responsibility to Congress, but gave it more power and emphasis. The creation of the CIA and the NSA seem to have missed this trend, however.

The 1970 Legislative Reorganization Act explicitly gave Congress the responsibility to review administrative policy to each standing committee.[34] In today's parlance, the goal was to be proactive rather than reactive. A new kind of oversight was thus born. Deering argued that this new oversight was more fully developed in the 1970s, when a popular expression in Congress was, "If we have to be in on the crash landings then we should be in on the takeoffs that precede them."[35]

Despite its short history, intelligence oversight does not differ from the norm insofar as it lacked significant oversight in its early days. The 1970s saw a renewed interest in oversight of many bureaucratic offices. In this sense, uncertainty in its inception and the predictable response of increased oversight do not seem to be extraordinary for intelligence oversight.

To compensate for not knowing the policy choices—or at least the thinking in the run-up to the decisions— legislators insist on sharing information. As has already been discussed with respect to the classification of intelligence agency documents, greater uncertainty leads to a need for greater information. McCubbins observed another element in that uncertainty. Specifically, he asserted that conflict among legislators—regarding the level of delegation at the original point of policy-making decision—increases the level of uncertainty. As a result, legislators will delegate greater amounts of policy-making responsibility to the bureaucratic agencies, thereby increasing the need for oversight at a later date.[36]

McCubbins concluded that increased conflict among legislators will result in decentralized oversight.[37] In other words, when information is scarce—or otherwise protected by the federal government—and members of Congress disagree over the ways to gain those information flows, congressional committees will be forced to resort to a reactive style of oversight, or fire alarm oversight.

For the intelligence oversight committees, information has been scarce. Information sharing was especially hard to come by at the time the committees were created. As for conflict, however, there have been very few public disagreements. In the era of trust, legislators largely agreed to oversee the intelligence apparatus in a limited way, deferring to the government agencies to conduct themselves within legal limits. During the investigations of the intelligence agencies, although some legislators debated the publicity of the hearings and the form of the response, there was little disagreement over the necessity of an inquiry.

There was a great deal of conflict in the run-up to the establishment of the intelligence oversight committees. The SSCI was created in 1976 with a vote of seventy-two to twenty-two. The HPSCI was created in 1977 with a vote of 227 to 171. In both chambers there was conflict about the creation of the committees, but the vote tallies reveal that the committees were in no real danger of not being created. House Republicans criticized the party ratio in the new committee, which reflected the party ratio of the entire House. They also questioned the new committee's ability to protect secrets. Liberal Democrats viewed the new committee as lacking sufficient tools of oversight.[38] Relying on McCubbins's characterizations, sufficient uncertainty and conflict suggest that intelligence oversight is most likely to receive traditional fire alarm oversight.

CONTEXT

According to Aberbach, the most important variable in determining the quality and quantity of congressional oversight is the context in which the legislators operate. "Congress responds to the changes in its environment."[39] Oversight became a significant goal for legislators in the 1970s throughout Congress because of public interest, resource scarcity, rivalries with the President, committee decentralization, and committee staff size—variables associated with

the House's 1973 Subcommittee Bill of Rights.[40] Aberbach perceived a positive result from these variables; they increase police patrol style oversight.

First, public interest in the subject of intelligence does not translate into congressional activity because intelligence has not proven especially salient. Foreign policy does not usually grab the public's attention. Granted, the post-9/11 investigations magnified public salience on this subject, but the secrecy surrounding the investigations generally made intelligence more obscure than other subjects grabbing public attention. On public salience, intelligence is a bit of a mixed picture. Certainly, large-scale scandals and investigations gain public attention and therefore congressional interest, although without front-page newspaper headlines, the topic of intelligence is certainly a low priority for the public.

Second, budget scarcity certainly affects intelligence oversight. Because its details are hidden within the defense budget, the intelligence budget can be limited by its defense counterparts. The defense oversight committees already have some jurisdiction over the intelligence agencies. By keeping the intelligence budget a secret and placing it within the defense budget, the jurisdictional boundaries between the committees get even murkier.

Third, Aberbach asserts that rivalries with the President influence the quality of oversight initiated by Congress. This kind of partisan scoring has been less prominent in the areas of foreign and defense policy. However, partisanship seems to be increasing. Public disagreements from the opposition party were common in the 1990s, producing a highly charged partisan atmosphere.[41] In the area of intelligence, partisanship increased as well. President Clinton faced a more partisan opposition even in areas of defense and foreign policy—traditionally supportive areas for the President.[42]

Finally, the intelligence oversight committees were a product of this increased interest in oversight. They benefited from the changes in the environment. However, one of the most prominent aspects of this change—the Subcommittee Bill of Rights—did not greatly affect the HPSCI and SSCI. These two Committees put more formal emphasis on the committee chairperson than the 1973 bill had demanded.[43] These Committees are more centralized than most of their counterparts. They remain a select committee with strong chairperson influence. They also have smaller staff sizes than other committees due to secrecy requirements.

Regarding Aberbach's four indicators, intelligence faces a murky picture. One factor, partisanship, encourages increased police patrol oversight, whereas the committee environment discourages it. Public interest and resource scarcity lead to mixed results in Aberbach's matrix. Intelligence seems to be both an attractive and a repulsive subject for oversight.

PERSONAL CALCULUS

Fenno determined that individual members of Congress consider their own personal goals in determining their objectives for congressional service. Fenno's

1973 research specified at least three goals for every House member that could be applied to all legislators: (1) reelection, (2) influence within the chamber, and (3) good public policy. Each member of Congress uniquely prioritizes these goals, and each chamber committee yields differing opportunities to achieve these goals. Insofar as each member may join a specific committee to achieve his or her own personal goals, the activities of the committee reflect these three individual objectives.[44]

For example, Fenno's research showed that congressmen seek committee assignments based on their prioritization of these three personal goals. Some committees are better at reelection opportunities than others which focus on power and prestige or policy and oversight. Thus some committees may offer oversight opportunities, and some congressmen may be motivated for personal reasons toward zealous oversight. Others may be less interested in policy goals, and are merely waiting until a more reelection-friendly committee assignment is available.

Members who expressed an interest in the Appropriations and Ways and Means Committees said that power or prestige were their top goals in seeking those committees. For members of the Post Office and Interior Committees, reelection was their top goal. They saw the ability to help their constituents through these committees as advantageous. Members of the Education and Labor and Foreign Affairs Committees expressed the third goal: good public policy.[45]

Foreign affairs or intelligence committees, such as the HPSCI and SSCI, are viewed as prestigious but not especially helpful in home district reelections. Such committees may provide opportunities to make good policy or to use as a platform for some other political ambition, but immediate reelection is not one of them.

David Mayhew's 1974 study of reelection habits supported the prevailing consensus that oversight receives a low priority among members of Congress. Elected legislators are interested in getting reelected. It is the "proximate goal of everyone, the goal that must be achieved over and over if other ends are to be entertained."[46] As a result, individual members of Congress try to engage in "credit claiming," the effort to encourage others to view them as responsible for some desirable activity in government. Similarly, legislators engage in "position taking" by publicly judging anything of interest to residents in their district.[47] Mayhew's election-minded member of Congress may be too preoccupied with fundraising, campaigning, or publicity-seeking activities to engage in behind-the-scenes oversight. Thus intelligence is unlikely to attract oversight.

COST-BENEFIT ANALYSIS

Relatedly, McCubbins and Schwartz argued that fire alarm oversight is more likely because it is less expensive and provides greater returns than police patrol oversight. Congress prefers decentralized, incentive-based oversight that utilizes cost-benefit analysis. Individuals are motivated to oversee administrative

decisions mostly based on reelection concerns. Even if legislators are motivated by public interest concerns, they are still more likely to choose the oversight that costs the least for the largest payback. In McCubbins and Schwartz's parlance, this is fire alarm oversight.

Intelligence certainly does not fit into the calculus of purely reelection-minded goals. At least before the events of 9/11, when intelligence was catapulted onto the front pages of all American newspapers, intelligence oversight had not created many opportunities for public speeches and easy claims for reelection bids. Even when the public is highly interested in intelligence, the secrecy demanded by its subject matter presents few options for credit claiming. Thus the cost-benefit analysis surrounding oversight of other administrative areas does not easily translate to the oversight of intelligence.

INTELLIGENCE OVERSIGHT

Intelligence oversight appears to be difficult to characterize using these nine academic criteria—information flows, committee history, subject matter/expertise, transparency, interest groups, uncertainty and conflict, context, personal calculus, and cost-benefit analysis. These diverse measures—at least within the modest descriptions given here—paint intelligence as both an attractive and a repulsive subject for oversight. Does this make intelligence oversight traditional or exceptional? Perhaps its varied characteristics will result in another murky picture here. Indeed, using the five dichotomies identified—latent and manifest, advocate and critical, centralized and decentralized, active and reactive, anticipatory and post hoc—intelligence oversight seems to fit a mix of traditional and exceptional oversight.

First, at first glance, the intelligence oversight committees seem likely to issue manifest legislation because their singular task is oversight. Ogul's distinction between manifest and latent oversight was one of formal and informal oversight. The intelligence communities received the direct attention of about half as many proposed bills from the House and Senate as bills related to Social Security in the 108th Congress.[48] The implication is that intelligence actually receives fewer manifest oversight efforts by Congress. Regarding latent oversight efforts, reporting requirements such as those from the inspector general in the CIA to Congress are quite prolific, according to Frederick Hitz, former inspector general at the CIA.[49] The other intelligence agencies do not have such requirements for their internally created inspectors general. However, other reporting requirements may be equally burdensome. Such a mix of latent and manifest oversight shows that there is no strong tendency for either in the oversight of intelligence.

Second, the intelligence oversight committees, although born out of criticism of the intelligence agencies, have been more friendly than not, according to Johnson.[50] Smist observed both friendly and critical oversight.[51] "Overseeing the intelligence community is like being a good parent. You have to encourage and

discipline," according to Representative Norm Dicks (D-WA) who has represented northwestern Washington for almost thirty years, including service on HPSCI.[52] Friendly or critical oversight is probably in the eye of the beholder, but the implication is that there is no single label that can be unquestionably applied to the oversight of intelligence.

Third, intelligence oversight attempts to be active, but it is mostly reactive. Representative Heather Wilson (R-NM) argued that the Committees are driven by crises but that this less-than-systematic approach is inherent in Congress's nature. The annual authorization/appropriation rhythm, the spikes of attention that surround events, and the interests of members drive all oversight, not just intelligence oversight.[53] Dicks agreed that the oversight agenda is event-driven, but he argued that the American culture is crisis-driven. "We like Monday-morning quarterbacking."[54] Any active oversight in the mold of police patrol oversight is hidden behind closed doors in regard to intelligence oversight. Reactive oversight efforts by the intelligence committees are quite public and easily measured. So, are these committees reactive or active? On the whole, they probably look like any other committee in terms of priority setting. If other committees are less likely to engage in active oversight, the intelligence oversight committees are also less likely to do so.

Fourth, the intelligence community is very decentralized. The oversight committees seem to mirror this diversity of agencies. The resulting multiplicity of hearings and committee meetings to which the agencies must respond seems very burdensome. On the other hand, some academic treatments of intelligence oversight have observed a domination of the chairperson of the committee. Indeed, the whole character of the oversight committees might fall on the mood established by the chairs.[55] As a result, the labels of *centralized* or *decentralized* do not seem well suited for intelligence oversight.

Finally, regarding the whole intelligence community, intelligence oversight is mostly post hoc because it is next to impossible to measure anticipatory oversight as defined by Ogul. It is not difficult to imagine some situations where anticipatory oversight has occurred. For instance, the unintended consequences in the wake of various oversight efforts to crack down on law breaking within the intelligence agencies has been risk aversion among the bureaucrats, according to some critics. Relatedly, it can be in the nature of a bureaucracy to produce risk-averse employees. This unintended consequence is not easily measured, but its existence seems to be taken for granted.[56] Congress's post hoc responsibility for oversight is obvious. When Congress established the CIA in 1947, it attached very broad parameters to that organization, requiring post hoc oversight in its future. Congress also recently reorganized the National Geospatial Intelligence Agency with very few ex ante pronouncements. Similarly, the Director of National Intelligence has some fairly broad parameters. The result is a post hoc necessity to ensure that the agencies provide information to Congress, respond to congressional attempts at reform, and follow more specific guidelines on front-page issues. The tools are reporting requirements, legislation, budgeting,

informal contacts, and public and private investigations. These are quite common.

Using these dichotomies, it appears that intelligence oversight follows some combination of traditional and exceptional oversight. It is both latent and manifest, both friendly and critical, both centralized and decentralized, but mostly reactive and post hoc. This indicates a tendency toward traditional oversight by the intelligence-related oversight Committees.

However, some attributes of the intelligence oversight system clearly appear unique—paramount secrecy, the term limits under which it has operated and continues to operate, the appointments process, and the history of intelligence oversight in the past. These characteristics are often the most publicly observable—and measurable—aspects of these committees.

First, secrecy plays a significant part in the character of intelligence oversight. Even though all government agencies protect their proprietary information, none assume the secrecy the intelligence agencies do. The rules for observing intelligence information in Congress are unique. Responsibility for intelligence information requires special clearances, restricts the access of staff to the information, and limits note taking. To read classified information from the intelligence agencies, legislators must move to another location altogether. Many choose not to do so. Although other committees have somewhat limited information flows as described herein, the HPSCI and SSCI do currently operate under unique rules. Whether they must have such unique rules is another question. This makes the current system of intelligence oversight unique.

Second, the intelligence oversight Committees have unique rules. HPSCI members abide by term limits, as did SSCI members until recently.[57] Members may serve on HPSCI for no more than eight years, although the chairperson has an unlimited tenure.[58] Until 2004, the SSCI term limit was also eight years. The rules of the committees also require that some portion of their membership simultaneously serve on the Armed Services, Appropriations, Foreign Relations, and Judiciary Committees.[59] These rules make the current system of intelligence oversight unique.

Third, the appointments process follows that of a select committee. These committees are generally set up on an ad hoc basis to address a specific question or problem. Since their inception, the intelligence oversight Committees have been select committees, making them unique even within the world of select committees. A select committee generally means that members are appointed directly by the chamber leadership for a short period of time. Members for standing committees are nominated by the party caucus and then appointed by the House or Senate leadership. According to one insider, selection for a "select" committee indicates a "sign of grace" from the leadership. "You look like one of the cool kids when you get picked."[60] Select committees have clout and prestige. The intelligence Committees, although they are select, are also "permanent," so they act like standing committees even though they are not. These attributes make the current system of intelligence oversight unique.

Finally, partisanship has historically been lacking on the intelligence oversight Committees. Members were originally selected to foster bipartisanship.[61] However, many critics have argued that partisanship on the Committees has increased in recent years.[62] This increase caught significant attention recently.[63] That such recent partisanship stands out suggests a uncommon history of bipartisanship. This makes the current system of intelligence oversight unique.

Intelligence oversight has been treated uniquely in the past. The intelligence committees follow both formal and informal rules that differ from other committees. They also follow both traditional and exceptional patterns of oversight. To illuminate the murky picture created by these academic treatments, the next question is whether intelligence oversight requires such unique approaches. To answer that inquiry, I turn to the participants themselves.

VIEWS OF THE INSIDERS: INTELLIGENCE OVERSIGHT NOT SO UNIQUE

"Like everything else in Congress, intelligence oversight is messy and imperfect," according to former Representative Charlie Wilson (D-TX).[64] Congressman Wilson served in the House for twenty-four years, representing east Texas. He is probably most remembered for supporting the Afghan resistance during the Cold War to such a degree that some argue he ran "his own war" out of the Appropriations Committee.[65] He argued that there is a general pattern in oversight that applies equally well to intelligence: Congress picks only one issue on which to focus. He said there is no systematic oversight; it is always dependent on the newspaper headlines.[66]

For similar reasons, former Representative Pete Geren concluded that intelligence oversight is "just like any other oversight. It is only when something goes wrong that the system really puts the subject into a crucible to examine it."[67] Geren (D-TX) served on the House Armed Services Committee during his eight-year tenure representing east Texas and currently serves as a special assistant to the Secretary of Defense. He conceded that when an issue like intelligence is shrouded in secrecy, congressional attention is particularly difficult to focus; but he explained that this is generally "the way oversight happens on all issues."[68]

Representative Heather Wilson agreed that HPSCI has a different atmosphere from other committees because of the seriousness of the issues, a sense of responsibility to the rest of Congress, and the additional work.[69] Wilson has represented central New Mexico for the past eight years. Her prior experience in Air Force Intelligence helped prepare her for service on the HPSCI. She remarked that the secrecy requirement presents a different constraint on the committee. Nonetheless, she concluded that "it is not different from any other oversight."[70]

Former Senator Richard Bryan (D-NV) agreed. His twelve years of service in the Senate and two years as vice-chair on SSCI gave him the opinion that intelligence oversight is just like any other oversight.[71] Similarly, former Senator

Malcolm Wallop (R-WY) said that intelligence oversight is same as any other oversight based on his eighteen years in the Senate, including membership on SSCI.[72]

Former Representative Timothy Roemer (D-IN) came to a slightly different conclusion based on his twelve years in the House of Representatives, including membership on HPSCI. "Oversight is not completely unique, but it is very different from oversight in the other committees."[73] He perceived as dissimilar the challenges and tools of intelligence oversight. Namely, the secrecy, the size and diversity of the budget, and the term limits make intelligence oversight somewhat unique. Nonetheless, in Roemer's opinion, the time constraints, the lack of long-range thinking, and the need for more systematic oversight apply equally to all congressional committees.[74]

VIEWS OF THE INSIDERS: UNIQUE OVERSIGHT

Senator Richard Shelby (R-AL) disagreed entirely. Shelby, based on his nearly thirty years of service in the Congress, including eight years in the House, called intelligence oversight unique. He also served as the chair or vice chair of SSCI for three terms (105th through 107th Congresses). He cited the secrecy, compartmentation, and "need to know" as the most distinct challenges of intelligence oversight. The result, in Shelby's opinion, is more work than any other committee. "Intelligence oversight is unique; it's more rigorous, active and involved" than any other committee.[75] In particular, Shelby focused on the reform of the intelligence agencies as such a large task that the Congress must work with the President to get any reform accomplished. He likened the transformation of intelligence to moving "an aircraft carrier down a creek."[76]

Former Senator Slade Gorton (R-WA) seized on the issue of secrecy as the origins of unique oversight. He argued that intelligence issues are "so difficult and so in the dark" that their oversight must be unique. Because the intelligence apparatus is not as transparent as other federal agencies, policy oversight of intelligence is unique.[77] Gorton represented Washington state for eighteen years, during which time he served on SSCI for only three years. He said he asked to leave the Committee because he did not think it was effective. The assignment was too time consuming, the topic was too obscure, and the secrecy prevented discussion in the home districts.[78]

CONGRESSIONAL PERSPECTIVES

This informal and unscientific survey of current and former representatives and senators showed that most believed intelligence oversight is not a unique undertaking. Only Gorton and Shelby argued that intelligence oversight is unique, mostly because of the challenges of secrecy. Their argument cannot be

dismissed lightly. The protection of sources and methods—a paramount goal for the intelligence agencies—necessitates certain rules peculiar to the intelligence committees. The requirement of a separate secure location to view certain information is particularly burdensome.

The remaining senators and representatives interviewed agreed that there are some distinct aspects to the task—secrecy in particular—but in the end, they mostly thought that intelligence oversight can be approached in the same way as oversight of other parts of the federal government. As found in the academic treatments of congressional oversight, this duty is often difficult, burdensome, and low on the scale of priorities for legislators. All subjects of oversight suffer from these challenges.

It is in Congress's constitutional power to perform oversight of the federal government. Its enumerated legislative powers, responsibility to declare war, provide for defense, oversee international commerce, and govern the power of the purse, justify oversight of intelligence.[79] Any efforts to increase the amount of scrutiny in any area of government to improve operations or ensure legal transactions would be welcomed by most senators and representatives. Senator Dennis DeConcini (D-AZ) argued that all oversight should be more stringent and more involved. Any legislation or other legislative tool that increases the attention given to the intelligence agencies would be a positive change, according to DeConcini (who represented Arizona for nearly thirty years and served as chair of SSCI from 1993–95).[80] Thus it is possible that any reform of intelligence oversight follow as a consequence of other oversight reform. Similarly, reformers of intelligence oversight may learn some lessons from the reform of other oversight subjects.

REFORM RECOMMENDATIONS

Starting with the broad recommendation to "strengthen congressional oversight of intelligence and homeland security," the 9/11 Commission advanced ten specific proposals for the reform of congressional oversight of intelligence:

1. Scrap the current system and replace it with either a joint committee or one committee in each chamber that combines authorizations with appropriations.
2. Make the intelligence budget public.
3. Grant subpoena authority to the committee or committees.
4. Institute subcommittees specifically dedicated to oversight.
5. The majority party representation should never exceed the minority representation by more than one.
6. Eliminate term limits.
7. If two committees are retained, downsize them.
8. Require that four members of this committee or committee simultaneously serve on the Armed Services, Judiciary, Foreign Affairs/

International Relations, and the Defense Subcommittee of the Appropriations Committee.
9. Staff should be nonpartisan.
10. Consolidate oversight of the Department of Homeland Security (DHS).[81]

Some of these recommendations stand alone; some work only in concert with the others. The first recommendation is the most radical. It is an entirely unique solution to the problems identified in the unity of the oversight of intelligence. Based on the literature review of the most important factors in determining the quality of congressional oversight, these solutions are not necessary. Moreover, none of the legislators interviewed for this research mentioned any inclination to such drastic measures. The Commission's theory was that "tinkering with the existing structure" would not produce the desired improvements. They advocated wholesale restructuring with the goal being to allow a small group of legislators the time and reason to master the intelligence system. It is not obvious, however, why such a radical response instead of a more limited modification—picking and choosing the most important reforms—is necessary to achieve these goals.

For instance, recommendations 3 through 10 could be accomplished with internal rules and probably very little debate. They are the most obvious changes and the least objectionable. In fact, they are not especially unique. Recommendation 3—subpoena authority—can be granted by a vote of the whole chamber and is already a part of some investigative subcommittees. Recommendation 4—investigative subcommittees—already exist in other committees in both the House and Senate. In fact, HPSCI and SSCI previously had investigative subcommittees. Recommendation 5 is not very different from the current system establishing the party ratio of each Congress at the start of the first session. Recommendation 6 has already been accomplished in the Senate. Recommendation 7 could easily be accomplished. To downsize a committee is somewhat against the mainstream. Most committees have been growing rather than shrinking, but it is not outside the usual realm of rules making authority in each chamber. Recommendation 8 is already part of the rules—both formal and informal—of HPSCI and SSCI. Recommendation 9 has been the goal from the start of the committees. Perhaps some new system might ensure a greater sense of nonpartisanship, but it is not a unique situation. Recommendation 10 would only require internal changes. This recommendation might be difficult considering the already murky state of oversight jurisdiction. Some other committees would have to give up their right to oversee this Department, but it could be done. These alterations could stand alone without any reference to the wholesale and very unique change of recommendation 1.

Recommendation 2 would require a change in the administration of intelligence, not an impossible task, but one that has encouraged heated debates in the past. Previous attempts to reveal the intelligence budget publicly and annually have proved unsuccessful. Though Commission members admit disclosure of a

number reveals very little, they nonetheless recommended the change in hopes it would foster accountability and allow observers to judge budgeting priorities. They further asserted that making the budget public would generally combat secrecy and complexity—elements that the Commission argue contributed to the series of mistakes behind 9/11.[82]

Contrary to recommendation 1, recommendations 2 through 10 would make intelligence oversight less unique. None of the remaining recommendations are as difficult or as unique as the first one. One unique problem to intelligence oversight—which was created at the very start of HPSCI and SSCI—is jurisdictional. Intelligence-oriented duties are spread throughout sixteen government agencies, and their oversight is spread through many congressional committees—intelligence, armed services, appropriations, international relations, judiciary, homeland security, and government reform.

This overlap requires the intelligence agencies to testify more often before Congress—a time-consuming endeavor—and before more and more committees. With the creation of the DHS and its responsibility to coordinate intelligence on domestic terrorist threats, the jurisdictional ambiguities multiplied. DHS leaders may appear before eighty-eight committees or subcommittees.[83] Thus the Commission recommended consolidation of DHS oversight in recommendation 10. The Commission did not touch on consolidation of intelligence oversight in general, however. It may be an even more daunting task with entrenched turf battles, but it is no less worthwhile to restructure the oversight of the other intelligence agencies. With jurisdictional ambiguity comes multiple responsibilities for the staff to canvass the status and opinions of other involved committees. The current system requires quite a lot of time-consuming checking and cross-checking, particularly regarding budgets.

The Commission's report quite clearly advocates the viewpoint that only a complete overhaul of the system will be helpful. According to the Commission members, choosing one or two of these recommendations without reforming the whole system would be insufficient. Their main argument was that decentralized, relatively weak, divided, superficial, unaccountable oversight contributed to the events of 9/11. These specific recommendations were meant to remedy those deficiencies to create a "strong, stable, capable" structure.[84] Aside from their first recommendation, however, they do not advocate particularly unique solutions. They advocated a wholesale overhaul without dividing that task into unique elements.

CONCLUSIONS

Congressional oversight can be labeled as such, or it can be included among other legislative or constituent-oriented efforts by members of Congress. Ogul argued that oversight can be a part of many of the activities of legislators, whether deliberate or not. He further found that these oversight efforts are more common and thus, for the purposes of this chapter, traditional.

Particularly in the budget process, congressional oversight may be deliberately and generally critical of federal administrations or play the part of the advocates for the government agencies. A committee might fight for an agency's budget to increase even while it is charged with overseeing that agency. In fact, Aberbach found that oversight is most often an advocate rather than a critic. This makes advocating style oversight more traditional than critical oversight.

Congressional oversight may attempt to anticipate events around the world and within the United States, or it may be content to react to these uncontrollable events. McCubbins and Schwartz found that legislators are most often reacting to events around them. This makes reactive oversight more traditional than anticipatory oversight.

Anticipatory oversight attempts to influence federal agencies with the threat of oversight, whereas post hoc oversight demands detailed reports to keep tabs on the administration of its broad mandates. McCubbins found that post hoc oversight is more common than its counterpart, and thus it is considered traditional here.

Using these dichotomies, it appears that intelligence oversight—in these academic characterizations—is a mix of traditional and exceptional oversight. Legislative efforts by the intelligence Committees are often manifest, but legislators also seem to choose informal, less deliberate efforts as well such as reporting requirements, relationships with the inspector general, and informal visits to the agencies themselves. The intelligence oversight efforts by Congress have followed a repeating pattern of advocacy followed by criticism. The intelligence-related Committees seem to be both centralized inside the Committees, but quite decentralized in terms of jurisdiction. Because international, often unpredictable events drive intelligence collection and analysis, they also drive intelligence oversight. So despite the efforts of some legislators to anticipate upcoming events and problems, the Committees are forced to be quite reactive. When creating oversight legislation—both manifest and latent—the Committees may have encouraged some unintended consequences. They have also provided some rather broad mandates to some of these agencies, causing the subsequent use of post hoc oversight tools. This combination of traditional and exceptional provides a very murky picture of the character of intelligence oversight.

Intelligence oversight, as it is currently organized, does operate under some unique oversight rules. Secrecy requirements, term limits, appointments, and bipartisanship do make intelligence oversight unique. Furthermore, the personal calculus and the related cost-benefit analysis of legislators serving on HPSCI or SSCI differs from those on other committees. There are fewer opportunities to benefit one's reelection campaign because the issues are not especially salient and the details are secret.

Relatedly, there are few interest groups in intelligence and very little transparency compared with other oversight subjects. The potential for greater public involvement in intelligence oversight is quite low. One potential exception is the public discussion of weapons of mass destruction in Iraq. Such salient issues do seem to arise every now and then, but typically, with few interest groups

to agitate for greater transparency, public demands for change are unlikely to aid congressional inquiries.

There are, however, some characteristics of intelligence oversight that are not especially unique. For instance, information flows from bureaucracies to Congress have been challenging in many areas of oversight. The number of classified documents has increased throughout the government, thus limiting congressional access to the information it needs for oversight. The response of Congress is to use reporting requirements on the bureaucratic agencies throughout the government.

Similarly, although intelligence presents a challenging learning curve, it is not so different from many defense or other technical areas of expertise. The details attending the appropriations to building an aircraft carrier, or following the labyrinthine world of the U.S. tax code are probably equally challenging.

Most important, the surrounding context of all congressional oversight is pervasive. The level of congressional interest in oversight of the federal agencies tends to ebb and flow with the greater political context, and intelligence oversight is no different. This leads to a level of uncertainty and conflict among legislators that is subject to the same outside influences as any other area of oversight.

Following this mixed picture about the unique character of intelligence oversight—both as it is currently practiced and as it compares to other oversight subjects—it may be useful to turn to the legislators themselves. In informal interviews, most of the interviewed representatives and senators involved in intelligence oversight claim it is not unique in comparison with other oversight demands. If their majority view is accurate, this suggests efforts to reform and improve on intelligence oversight structures likewise need not be exceptional. Thus new and reformed congressional efforts to oversee intelligence can follow the same paths of improvement as other oversight efforts. Rather than turn to unique solutions, it may be equally fruitful to study other forms of oversight to find effective solutions to some unique and some not so unique problems.

NOTES

This chapter stems from a paper presented at the International Studies Association (ISA) annual meeting in San Diego, CA, 2006.

1. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United State* (New York: Norton, 2004), p. 419. As of 2006, the intelligence community includes sixteen agencies: Central Intelligence Agency (CIA), Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency (NSA), Air Force Intelligence, Army Intelligence, Coast Guard Intelligence, Marine Corps Intelligence, Navy Intelligence, and elements of the Department of Energy, the Department of Homeland Security, the Department of State, the Department of the Treasury, the Drug Enforcement Agency, and the Federal Bureau of Investigation (FBI).

2. Ibid., p. 420. Some suggestions were: possibly a joint House-Senate committee or a combination of authorization and appropriations in one committee, an end to term limits

in the intelligence oversight committees, a public budget for the intelligence community, subpoena power for the committee members, oversight subcommittees, joint service with related committees for the HPSCI and SSCI members, and a smaller committee to encourage a greater sense of responsibility among committee members.

3. Morris Ogul, *Congress Oversees the Bureaucracy* (Pittsburgh, PA: University of Pittsburgh Press, 1976), p. 180.

4. Joel Aberbach, *Keeping a Watchful Eye: The Politics of Congressional Oversight* (Washington, DC: Brookings Institution, 1990), p. 173.

5. Mathew McCubbins and Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms," *American Journal of Political Science* 28 (1984), p. 176.

6. Morris S. Ogul and Bert A. Rockman, "Overseeing Oversight: New Departures and Old Problems," *Legislative Studies Quarterly* 15 (1990), p. 13. The authors credited Aberbach's 1987 review of McCubbins and Schwartz's 1984 article for the original idea of active versus reactive oversight. Ogul and Rockman further refined the concept in this 1990 literature review. See Joel Aberbach, "The Congressional Committee Intelligence System: Information, Oversight, and Change," *Congress and the Presidency* 14 (1987), pp. 51–76.

7. Ogul and Rockman, "Overseeing Oversight," pp. 7, 21.

8. Reactive oversight is distinct from post hoc oversight insofar as it is those efforts that react to outside events beyond the control of individuals, such as natural disasters, acts of terrorism or war, or public scandals. Post hoc oversight refers to the efforts of Congress to control the administrative duties it delegated to a federal agency. In other words, post hoc oversight is necessary to ensure that government agencies act in the way that Congress intended.

9. Anticipatory oversight is distinct from ex ante oversight insofar as it is those efforts that attempt to anticipate outside events beyond the control of individuals. Ex ante oversight is the deliberate, detailed instructions that Congress gives to federal agencies in their creation. When legislators delegate some authorities to government offices, they may be very specific in their guidance (ex ante oversight) or somewhat vague, preferring to look over the shoulders of administrators as they go about the business of broad mandates (post hoc oversight).

10. See for instance, Ogul, *Congress Oversees the Bureaucracy*; Seymour Scher, "Conditions for Legislative Control," *Journal of Politics* 25, no. 3 (1963).

11. Aberbach, *Keeping a Watchful Eye*, p. 190.

12. Christopher J. Deering, "Alarms and Patrols: Legislative Oversight in Foreign and Defense Policy," in Colton C. Campbell, Nicol C. Rae, and John F. Stack Jr., eds., *Congress and the Politics of Foreign Policy* (Upper Saddle River, NJ: PrenticeHall, 2003), p. 134.

13. Ibid.

14. Aberbach, *Keeping a Watchful Eye*, p. 74.

15. Arthur Lupia and Mathew McCubbins, "Learning from Oversight," *Journal of Law, Economics, and Organization* 10 (1994), p. 112. According to the authors, the objective of the legislators is to create institutions that produce learning from oversight. Without this important knowledge from bureaucratic insiders, legislative delegation of authority to government agencies is tantamount to abdication of congressional responsibilities.

16. A quick glance at the websites of these offices reveals the differences. Of course, the Consumer Products Safety Commission and the surgeon general have a primarily

public function, and they attempt to reach as many Americans as possible. Each of the intelligence community members has a website with publicly available information, but far more of their work is quite clearly classified.

17. See generally L. Britt Snider, *Sharing Secrets with Lawmakers: Congress as a User of Intelligence* (McLean, VA: Center for the Study of Intelligence, CIA, 1997), available at http://www.cia.gov/csi/monograph/lawmaker/toc.htm on (accessed February 18, 2006).

18. See U.S. House, Permanent Select Committee on Intelligence, *Publication of the Rules for the Permanent Select Committee on Intelligence* (108; June 12, 2003) (Washington, DC: Library of Congress). Text from *Congressional Record.* Available from Thomas (online service).

19. Scott Shane, "Increase in the Number of Documents Classified by the Government," *New York Times*, July 3, 2005, available at http://www.nytimes.com/2005/07/03/politics/03secrecy.html?ex=1278043200&en=cf5505f95e78680a&ei=5088&partner=rssnyt&emc=rss (accessed February 18, 2006). These classifications are somewhat nebulous, as when labels such as "sensitive security information" are employed.

20. Frank J. Smist, *Congress Oversees the U.S. Intelligence Community*, 2nd ed. (Knoxville: University of Tennessee Press, 1994), pp. 21–24.

21. Scher, "Conditions for Legislative Control," p. 540.

22. Aberbach, *Keeping a Watchful Eye*, p. 162.

23. Charles R. Shipan, "Congress and the Bureaucracy," in Paul J. Quirk and Sarah A. Binder, eds., *The Legislative Branch* (New York: Oxford University Press, 2005), pp. 438–45. Although the legislative veto was declared unconstitutional in *INS v. Chadha* (1983), Congress generally retains the right of congressional review of agency rules. In the Congressional Review Act of 1996, Congress asserted the ability to "disapprove" of certain agency decisions with a congressional joint resolution.

24. Ogul, *Congress Oversees the Bureaucracy*, p. 14.

25. HUMINT is an abbreviation for human intelligence or the people who spy for the United States. SIGINT stands for signals intelligence, a catchall phrase including the collection of conversations by phone or other technical means usually collected by satellite. IMINT is an abbreviation for imagery intelligence—the photography or digital imagery usually collected by satellite.

26. Ogul, *Congress Oversees the Bureaucracy*, p. 14.

27. HPSCI reviews matters related to the National Foreign Intelligence Program (NFIP), Tactical Intelligence and Related Activities (TIARA), and Joint Military Intelligence Programs (JMIP). NFIP, TIARA, and JMIP are budgetary categories for the funding streams into the intelligence community. NFIP includes approximately half the intelligence budget and consists of the civilian parts of the community: the CIA and all its parts; the Director of Central Intelligence; the Bureau of Intelligence and Research in the Department of State; the National Security Agency (NSA); the National Geospatial Intelligence Agency; the Department of Homeland Security (DHS) since 2002; the National Reconnaissance Office; the FBI; the Department of the Treasury; and the Department of Energy intelligence offices; and half of the Defense Intelligence Agency (DIA). JMIP funding covers the defense-related intelligence efforts that do not belong to any one branch of the armed services: half of the DIA, and parts of DOD intelligence offices. TIARA covers the armed services' intelligence branches. The House Armed Services Committee (HASC) shares jurisdiction with HPSCI on TIARA and JMIP as well as the Department of

Energy. HPSCI has exclusive jurisdiction over the NFIP. HASC's responsibilities cover a wide range of defense-related issues. Intelligence is just one small part of its agenda. SSCI also has some responsibility for NFIP, JMIP, and TIARA-related funding, activities, and organizations. However, the Senate Armed Services Committee (SASC) holds exclusive jurisdiction over TIARA and JMIP. Jurisdiction over NFIP is shared by SSCI and SASC. Again, SASC's jurisdiction is so broad that intelligence can only be a small part of it. As such, intelligence only occupies part of the time of the senators on SASC.

28. Ogul, *Congress Oversees the Bureaucracy*, p. 15.

29. Shipan, "Congress and the Bureaucracy," p. 453.

30. Mathew D. McCubbins, "The Legislative Design of Regulatory Structure," *American Journal of Political Science* 29 (1985), p. 737.

31. Loch K. Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (Lexington: University of Kentucky Press, 1985), p. 7. From its inception in 1947, the CIA was allowed to operate almost completely freely, while Congress's inquiries resembled friendly support—and even awe—rather than meaningful query. The House and Senate Committees on Armed Services and Appropriations oversaw CIA activities. Among these four committees, the CIA was subjected to about twenty-four hours of legislative hearings per year for most of the 1950s and 1960s.

32. Loch K. Johnson, "Accountability and America's Secret Foreign Policy: Keeping a Legislative Eye on the Central Intelligence Agency," *Foreign Policy Analysis* 1 (2005), p. 106.

33. P.L. 79-601 (Legislative Reorganization Act of 1946).

34. P.L. 91-510 (Legislative Reorganization Act of 1970).

35. Deering, "Alarms and Patrols," p. 129.

36. McCubbins, "The Legislative Design of Regulatory Structure," p. 738.

37. Ibid., 739.

38. Smist, *Congress Oversees the U.S. Intelligence Community*, pp. 82, 214–16.

39. Aberbach, *Keeping a Watchful Eye*, p. 104.

40. In this legislation, subcommittees were authorized to meet on their own authority, set their own rules, and enact their own legislation. Thus more incentives to oversee administrative policy evolved.

41. Joel D. Aberbach, "What's Happened to the Watchful Eye?," *Congress and the Presidency* 29 (Spring 2002), p. 19.

42. Stephen F. Knott, "The Great Republican Transformation on Oversight," *International Journal of Intelligence and Counterintelligence* 13 (2000), p. 49.

43. Smist, *Congress Oversees the U.S. Intelligence Community*, p. 217.

44. Richard F. Fenno Jr., *Congressmen in Committees* (Boston: Little, Brown, 1973), pp. 1–2. Fenno studied six committees from the House from 1955 to 1966. These are committees on Appropriations, Education and Labor, Foreign Affairs, Interior and Insular Affairs, Post Office and Civil Service, and Ways and Means. Fenno also briefly examined their Senate counterparts.

45. Ibid., pp. 3–9.

46. David R. Mayhew, *Congress: The Electoral Connection* (New Haven, CT: Yale University Press, 1974), p. 16.

47. Ibid., pp. 49–61.

48. A quick glance by the author at the bills listed in Thomas, an online research service from the Library of Congress, shows these results.

49. Frederick Hitz, interviews with the author, Alexandria, VA, August 18, 2001, and September 12, 2003.

50. See generally Johnson, "Accountability."

51. See generally Smist, *Congress Oversees the U.S. Intelligence Community*.

52. Representative Norm Dicks, interview with the author, October 15, 2003, Washington, DC.

53. Representative Heather Wilson, interview with the author, November 9, 2003, Washington, DC.

54. Dicks interview.

55. Smist, *Congress Oversees the U.S. Intelligence Community*. This kind of personal importance was echoed in an interview conducted by the author with L. Britt Snider, former inspector general of the CIA from 1998 to 2001. Snider said he was struck by how the whole system is still personality-driven. Britt Snider, interview with the author, June 25, 2001, Arlington, VA.

56. Richard A. Posner, "The Danger in 'Fixing' the CIA," *Los Angeles Times*, May 24, 2005, p. B13.

57. In its original documents, the SSCI term limit was eight years. This limit changed in 2004. See Senate, *A Resolution to Eliminate Certain Restrictions on the Service of a Senator on the Senate Select Committee on Intelligence*, 108th Congress, 2nd sess. (2004), S.R. 445.

58. *Rules of the House of Representatives* (109th Congress), 532 (Rule X: Organization of Committees, clause 12k).

59. *Rules of the House of Representatives* (109th Congress), 519 (Rule X: Organization of Committees, Clause 11a) and *Senate Resolution 400* (*Rules of Procedure for the Select Committee on Intelligence, United States Senate*), as amended May 19, 1976, available at http://intelligence.senate.gov/rules%20of%20procedure.htm (accessed March 30, 2006).

60. Mark Lowenthal, interview with the author, February 16, 2006, by phone.

61. Smist, *Congress Oversees the U.S. Intelligence Community*, p. 83.

62. Dana Priest, "Congressional Oversight of Intelligence," *Washington Post*, April 27, 2004, available at http://www.washingtonpost.com/ac2/wp-dyn/A44837-2004Apr26?language=printer (accessed February 21, 2006).

63. L. Britt Snider, "Congressional Oversight of Intelligence after September 11," in Jennifer E. Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005), p. 242.

64. Representative Charlie Wilson, interview with the author, July 1, 2004, Washington, DC.

65. See generally, George Crile, *Charlie Wilson's War: The Extraordinary Story of the Largest Covert Operation in History* (New York: Atlantic Monthly Press, 2003).

66. Charlie Wilson interview. The result, according to Wilson, is that much of the intelligence community escapes oversight.

67. Representative Pete Geren, interview with the author, April 26, 2004, Arlington, VA.

68. Ibid. The result, according to Geren, is that legislators must trust the intelligence agency professionals because they cannot see so much of what goes on.

69. Charlie Wilson interview.

70. Ibid.

71. Senator Richard Bryan, interview with the author, November 3, 2003, by phone.

72. Senator Malcolm Wallop, interview with the author, October 16, 2003, by phone.

73. Representative Timothy Roemer, interview with the author, March 15, 2004, by phone.

74. Ibid.

75. Senator Richard Shelby, interview with the author, April 2, 2004, Washington, DC.

76. Ibid.

77. Senator Slade Gorton, interview with the author, September 26, 2003, by phone.

78. Ibid. The result, according to Gorton, was that the intelligence community runs itself.

79. David Everett Colton, "Speaking Truth to Power: Intelligence Oversight," *University of Pennsylvania Law Review* 134 (December 1988), p. 578.

80. Senator Dennis DeConcini, interview with the author, March 6, 2006, by phone.

81. *The 9/11 Commission Report*, pp. 420–21.

82. Ibid., p. 416.

83. Ibid., p. 421

84. Ibid., p. 416.

7

INTELLIGENCE ACCOUNTABILITY

A Comparative Perspective

HANS BORN AND IAN LEIGH

THIS CHAPTER PRESENTS A COMPARATIVE SURVEY OF the accountability for intelligence. Space does not permit an extended description and analysis of the arrangements in different countries.[1] Instead, after a brief historical overview, we take a thematic approach. This emphasizes four factors: the importance of accountability within an agency itself; the role of the executive in accountability; the place of parliamentary or legislative oversight; and finally, independent complaints, inspection, and audit processes.

If spying is the second oldest profession, intelligence accountability is by comparison a modern development. For practical purposes the story begins in the mid-1970s with the official exposure and cataloging of abuses in the U.S. intelligence community by the Church and Pike Committees.[2] This established a pattern for scandal followed by reform that has been repeated in many countries. Similar investigations followed in Canada (the McDonald Commission, 1977–80), Australia (the Royal Commission under Justice Hope, 1974–77), and Norway (the Lund Commission, 1996).[3]

Investigations such as these launched a movement of reform that has steadily spread democratic oversight concerns from the United States to Australia and Canada in 1979 and 1984, respectively, and, within Europe, to Denmark in 1988, the United Kingdom in 1989, Austria in 1991, Greece in 1994, Norway in 1996, and Italy in 1997.[4] So firmly is this now established as part of the good governance agenda that the need for effective democratic oversight has received the backing of international bodies such as the Parliamentary Assemblies of the Council of Europe and of the Western European Union.[5]

The collapse of the Soviet bloc and the resulting constitutional reforms in Eastern and Southern Europe launched another wave of reform. Alongside the

establishment of civilian democratic control over the military, there have been established in most of these transitional democracies parliamentary committees whose responsibility is the oversight of the security and intelligence agencies. This was the case for example in Romania, Slovenia, Lithuania, Estonia, Croatia, and Bosnia-Herzegovina. [6] Outside the Anglo-Saxon world and Europe reform has spread also to such transitional countries as South Africa,[7] Argentina,[8] and South Korea.[9]

In these transitional states the domestic security agency had often been tainted by a repressive past. Even among more established liberal democracies, however, there has been a growing recognition that security and intelligence agencies can potentially threaten as well protect democracy. If left unregulated, the propensity of these agencies to systematically invade individual privacy by information gathering and surveillance; manipulate the political process by infiltrating political movements, pressure groups, and trades unions; engage in psychological operations and disinformation; or even, in extreme cases, effect political assassinations and coups in foreign countries is now well documented.

Alongside preventing scandal and cementing constitutional change, a third reason for the spread of intelligence accountability can be mentioned: respect for the rule of law. The absence of an explicit legal basis for the work of its security and intelligence agencies may bring a state into conflict with constitutional or human rights norms, especially where powers affect individuals, for example, surveillance. This has been of particular importance in leading to reform in European states that are parties to the European Convention on Human Rights.[10] In several European states, aspects of the legal basis have been found to be inadequate.[11] This has prompted the passing of legislation that in turn gives security and intelligence agencies legitimacy. In the process, legislators have used the opportunity to address the principles that should govern this important area of state activity and lay down limits to the work of such agencies.

Three recurring issues in the design of oversight procedures can be mentioned at this point. First is the need to establish mechanisms to prevent political abuse while providing for effective governance of the agencies. Overall, the objective is that security and intelligence agencies should be *insulated* from political abuse without being *isolated* from executive governance. Second is upholding the rule of law in the sense of subjecting the agencies to legal control. As in other areas, one key task of the legislature is to delegate authority to the administration but also to structure and confine discretionary powers in law. Third, many countries have been concerned to ensure that the exceptional powers granted to the agencies (such as surveillance and the gathering of personal data) are used in a way proportionate to the threat as a means for protecting civil rights.

With these preliminary remarks in mind we turn to the specific role of the agency, the executive, parliament, and independent review bodies in intelligence accountability.

THE ROLE OF THE AGENCY

The executive and parliament depend for their oversight functions on loyal and professional intelligence agencies. Without a professional agency acting in a disciplined manner, reporting and accountability mechanisms will not function accurately or not at all. Therefore, it is vital that any accountability framework sees the agency not only as an object of control but also as a constituting element of the accountability framework. Furthermore, the internal functioning and organization of the agency is also the first "firewall" against human rights violations by agency officials. Proper mandates, codes of conduct, and other regulations as well as internal complaint mechanisms diminish the risk that officials will be engaged in human rights violations. The focus is here on four important elements of the internal functioning of intelligence agencies: defining the mandate, appointing the director, the use of special powers, and internal direction.

Defining the Mandate

A key aspect of accountability for security and intelligence agencies is that their role and sphere of operation are clearly defined. Therefore, countries that introduced intelligence accountability (as mentioned in the introduction) have enacted legislation to this effect, that is, emphasizing that responsibility for delineating the tasks of a security or intelligence agency lies with parliament and that this role should not be changed without reference to legislators. In transitional states particularly, this may help provide protection from abuse of the agencies by the government. A legal basis is also necessary because of the exceptional powers with which these agencies are often entrusted.

It is also important that security and intelligence agencies are differentiated from other institutions, such as law enforcement bodies, and the legislative mandate can help do so, as is the case in Germany where the *Trennungsgebot* (firewall) is in place between police, military, and intelligence services. Failure to make these clear distinctions will lead to blurred lines of accountability, and to the risk that the special powers that security and intelligence agencies possess are used in routine situations where there is no imminent threat to the state. Post-transition states in particular, for example, Bosnia-Herzegovina, have found it important to clarify, by means of detailed legislation, the various aspects of national security—rather than leaving the mandate of the security and intelligence agencies essentially open-ended through the use of phrases such as "protecting the security of the state."[12]

Four different type of agencies can be distinguished on the basis of the mandate: internal (domestic) service, external (foreign) service, collection and analysis of information services, as well as services that act to counter domestic or foreign security threats. With regard to the first two types, it seems common practice to refer to "intelligence services" for agencies with foreign mandates and to "security services" for agencies with domestic mandates. Both intelligence

services and security services can have either a more proactive mandate or be restricted to the gathering and analysis of information. Combining these factors, several different types of institutional arrangements have been adopted by states:

a. A single agency for security and intelligence (both domestic and external), for example, Bosnia and Herzegovina, the Netherlands, Spain, and Turkey.
b. Separate agencies for domestic and external intelligence and security, with either separate or overlapping territorial competences, for example, the United Kingdom, Poland, Hungary, and Germany.
c. A domestic security agency but no acknowledged or actual foreign intelligence agency, for example, Canada.

In post-authoritarian societies, there are often strong memories of security and intelligence services endowed with broad mandates and sweeping powers used to protect dictatorial regimes against rebellions from their own people. Services were used by such regimes to suppress political opposition to prevent any kind of demonstration and eliminate leaders of labor unions, the media, political parties, and other civil society organizations. In doing so, the services intervened deeply in the political and daily life of the citizens. After the transition to democracy, the new leaders were determined to curtail the mandate and powers of the services and guarantee its political neutrality. An example of this practice is given by the Argentine National Intelligence Law of 2001. This law forbids the services to work in areas where they used to be active under the Generals' regime, that is, they are forbidden to be involved in repressive activities; process information on individuals on the basis of race, political ideology, religion, or membership of a trade union or exert influence over the political situation and media in Argentina.[13]

Appointing the Director

A key aspect of the legislation governing intelligence and security agencies is the process for appointing the director. Personal qualities of leadership, integrity, and independence are necessary in the person appointed. This will inevitably be a senior official position, and it is important that the process of appointment reinforces and guarantees the status of the position.

Various countries have adopted the minimum standard that the appointment should be open to scrutiny outside the executive. Constitutional traditions vary, however, in how this takes place in the case of senior government posts. In some countries (for instance, the United Kingdom) the safeguards against abuse rest on customary practice, which, if they were broken, would lead to political criticism and possible censure by independent officials. In other states, a formal confirmation or consultation procedure is common, which enables the legislature to either veto or express their opinion on an appointment. This may be underwritten

by a constitutional requirement either that official appointments must be approved by parliament or, alternatively, that they can be blocked by a parliamentary vote (e.g., the practice in the United States). A parliamentary verdict of nonagreement on a proposed nominee may not have the de jure consequences of a veto vote, but often it will de facto. Other noteworthy practices can be found in Belgium, Australia, and Hungary. In Belgium, the director-general is obliged to take the oath before the chairman of the Permanent Committee for Supervision of the Intelligence and Security Services before taking office.[14] In Australia, the prime minister must consult with the leader of the opposition in the House of Representatives concerning the proposed appointment.[15] Considering the executive's involvement in the appointment of the director, the Hungarian law is of interest because it addresses the role of both the respective minister and the prime minister.[16] The goal of all these and similar provisions is to achieve a broad political consensus for the director's appointment.

Apart from the appointment process, in various countries safeguards exist against both improper pressure being applied on the director and abuse of the office. Provisions for security of tenure, subject to removal for wrongdoing, are therefore common, as demonstrated by the legislation example from Poland.[17]

Internal Direction and Control

Essential safeguards within an agency should exist to ensure legality and propriety with regard to its functioning. Inevitably, it is impossible to spell out in legislation every matter of detail concerning the operation of a security and intelligence agency. Moreover it may be undesirable to do so where this would give public notice of sensitive operational techniques. Nonetheless various countries have adopted agency procedures to prevent abuse and offences. In the context of accountability mechanisms, the focus here is on reporting on illegal action and code of conduct.

The most reliable information about illegal action by a security or intelligence agency is likely to come from within the agency itself. Hence, a duty to report illegal action and to correct it is useful and also strengthens the position of staff within the agency in raising concerns that they may have about illegality. For example, the U.S. Department of Defense has created an internal channel for reporting questionable or improper intelligence activities to the assistant secretary of Defense (Intelligence Oversight) and the general counsel.[18] The same is true of so-called whistle-blower provisions, which give protection from legal reprisals to such persons when they raise issues of this kind with the appropriate oversight bodies. In Bosnia and Herzegovina, an employee who believes that he received an illegal order should draw the attention of superior, insist on written confirmation, and eventually report to the next layer of authority.[19] In Hungary, the director-general of the National Security Service is obliged to report unlawful acts immediately to the minister and to the National Security Committee in Parliament.[20] Additionally, staff should be protected in reporting illegality from both disciplinary action and

criminal prosecution. A detailed illustration of a public interest defense to criminal liability for unauthorized disclosure protection can be found in Canada.[21]

The formulation of an internal code of conduct is another important manner to ensure proper behavior on the part of intelligence officials. To devise a professional code of ethics and offer training courses for intelligence staffers are useful means to set, communicate, and maintain a minimum level of shared practices among intelligence employees. For example, in the United States, the assistant to the secretary of Defense (Intelligence Oversight) is tasked with, among other issues, the institutionalization of the orientation, awareness, and training of all intelligence personnel in intelligence oversight concepts (e.g., upholding the rule of law, protection of statutory and constitutional rights of U.S. persons).[22] The Republic of South Africa opted for a code of conduct for intelligence workers that gives clear guidance on the ethical scope of their activities.[23]

The Use of Special Powers

Some intelligence bodies are solely concerned with reporting and analysis, for example, the Office of National Assessments in Australia, the Information Board in Estonia, and the U.K. Joint Intelligence Committee. However, where security and intelligence agencies have a proactive, information-gathering capacity they will usually be granted specific legal powers, all the more so where their role includes countering or disrupting threats to national security, actively gathering intelligence, or law enforcement in the field of national security. "Special powers," therefore, refers to the granting of enhanced powers to security and intelligence agencies that directly affect civil liberties, including conducting surveillance and recording information, searching enclosed (private) spaces and objects, using stolen or false identities, monitoring conversations and data transfer, requesting cooperation from providers and public telecommunication networks, as well as having access to all places for installing observation equipment.[24] Typically, greater powers are granted than those normally available to the police or other law enforcement bodies because threats to security are seen to be more serious than ordinary criminality.

Because of the dangers for the rule of law and human rights, the agency's use of special powers needs to be overseen. Helpful practical guidance on what this means in relation to one area of importance—surveillance—was given by the Canadian McDonald Commission of inquiry into abuses by the Royal Canadian Mounted Police, which reported in 1980. To ensure the protection of privacy from intrusive surveillance, the McDonald Commission proposed the following four general principles: the rule of law should be strictly observed; investigative techniques should be proportionate to the security threat under investigation and weighed against the possible damage to civil liberties and democratic structures; less intrusive alternatives should be used wherever possible; and control of discretion should be layered so that the greater the invasion of privacy, the higher

the level of necessary authorization.[25] A fifth point should be added to these principles: legislation governing exceptional powers should be comprehensive. If the law covers only some of the available techniques of information-gathering there will be an in-built temptation for an agency to resort to less regulated methods (for instance those that do not require approval outside the agency itself). Examples of comprehensive legislation can be found, for instance, in Germany, the Netherlands, and the United Kingdom.[26] It is noteworthy that the latter cover not only surveillance but also gathering information through human sources.

Prior to surveillance or information gathering, many systems require the authorization of the use of special powers by a person external to the agency. This may be a judge (as in Bosnia and Herzegovina, Estonia, and Canada) or a specialized court (for example in the Netherlands under the Intelligence and Security Services Act or the United States under the Foreign Intelligence Surveillance Act of 1978) or a minister (e.g., the United Kingdom). In the latter case, because a minister is part of the executive, it is important that proper controls against political abuse exist. In Germany, the law requires that the minister not only approve the use of special powers but also report them to the parliamentary committee on intelligence oversight.[27]

THE EXECUTIVE

The importance of the security and intelligence services in supporting the governments of modern states with the supply and analysis of relevant intelligence to counter specified threats and advance domestic, defense, and foreign policy is undeniable. This is equally true of domestic security (especially counterterrorism, counterespionage, and countering threats to the democratic nature of the state), as well as in the realm of international relations, diplomacy, and defense. This pressing need means that the executive branch is entitled to expect unswerving loyalty from the agencies in implementing the policies of the government in the nation's interests.

Clear executive control of the agencies is also the antidote to the possibility of the agencies becoming a law unto themselves in a way that is antidemocratic and creates a vacuum of accountability. In fact one can go further and argue that, without information or control, the executive cannot itself be properly accountable to the public within a balanced constitution.

A delicate line must be walked, however, in avoiding the equal and opposite error that with unchecked executive control governments may be tempted to use security agencies or their exceptional powers and capacities to gather information for the purposes of domestic politics, for instance, to discredit domestic political opponents. Sensitive accountability structures, therefore, attempt to insulate security and intelligence agencies from political abuse without isolating them from executive governance.

Executive Control in Various Political Systems

The precise form that executive accountability takes in any given country is necessarily relative to the prevailing constitutional arrangements. The differences between presidential executives like the United States, dual executives like France, or Westminster-style parliamentary executives, of course, profoundly affect both the distribution of responsibility for security and intelligence and the corresponding oversight arrangements Even within one type of system, wide variations may exist. For example, quite different patterns of oversight for security and intelligence have emerged in the Westminster family of the United Kingdom, Australia, Canada, and New Zealand.[28]

It is common to find that on the ministerial side, intelligence laws deal with the allocation of responsibility for formulating policy on security and intelligence matters (within, of course, the legislative mandate of the agencies). The laws address, as well, the right to receive reports from the agencies; a reservation of the right to approve matters of political sensitivity (e.g., cooperation with agencies from other countries)[29]; or activities that affect fundamental rights (such as the approval of the use of special powers, whether or not additional external approval is required, for instance, from a judge). Conversely, on the agency side, the following corresponding duties may be codified: the duty to implement government policy, the duty to report to ministers, and the duty to seek approval of specified sensitive matters.

In pure presidential and parliamentary executive systems, however, the safeguards are more likely to take the form of a series of legal checks and balances. These may include security of tenure for the agency heads, legal limits to what the agencies can be asked to do, and independent mechanisms for raising concerns about abuses (e.g., safe routes for whistle-blowing outside the agency for staff who fear improper political manipulation).

At the institutional level the checks and balances model between the executive, the legislature, and the judiciary is, of course, a design feature of the U.S. Constitution. In the intelligence field it takes the form both of powerful congressional committees whose rights extend to timely information about intelligence operations and the blocking powers of the purse and legal controls over the agencies.

Within Westminster-style parliamentary executives, the notion of ministerial accountability to Parliament underpins the design of accountability structures. Effective parliamentary oversight presupposes effective control of the agencies by ministers. Parliaments can only reliably call ministers to account for the actions of the intelligence agencies if ministers have real powers of control and adequate information about the actions taken in their name.

In each of these three systems, however, there are prudential reasons to make a separation between executive oversight and managerial control of the agencies and their operations. If political leaders are too closely involved in day-to-day matters, it will be impossible for them to act as a source of external control, and

the whole oversight scheme will be weakened. Equally, if executive control is too close, there is the danger of politicizing the intelligence cycle, especially at the analysis stage, and the end product will be less useful as a consequence.[30] Effectiveness, therefore, suggests distinct but complimentary roles for the executive and agency heads. One provision articulating this principle is the Canadian Security Intelligence Service Act 1984, which refers to the director of the Service having "the *control and management* of the Service" that is "under the direction" of the minister.[31] The Polish intelligence legislation similarly clearly distinguishes between the respective competences of the prime minister and the heads of the agencies.[32]

Transitional societies, wherein previously the line between civilian government and intelligence agencies has been blurred, may find it necessary to provide detailed prohibitions to prevent future executive or ministerial abuses. For instance, in the new Bosnia-Herzegovina legislation, while the chair of the Council of Ministers has a number of detailed policy and review functions,[33] under article 10 he or she is expressly prevented from assuming "in whole or in part" "the rights and responsibilities" of the director-general or deputy director-general. Conversely, the director-general's rights and responsibilities are detailed in a way that makes clear their day-to-day managerial character; these include preparation of the annual budget of the agency; directing analytical, technical, administrative, and partnership cooperation operations; and the external operations of the agency. The same provision lists also protecting intelligence sources, intentions, and operations from unauthorized disclosure as well as obtaining, through the chair, approval and support from the minister of Foreign Affairs for activities that may have a serious impact on the foreign policy of Bosnia and Herzegovina.

Ministerial Knowledge and Control of Intelligence

Within a healthy constitutional order, ministers needs a sufficient degree of control over intelligence agencies and the right to demand information from them to discharge their responsibilities as members of an elected executive acting on behalf of the public. They also need to have adequate control and information to be able to account to parliament for the agencies' use of their legal powers and their expenditure. Effective democratic control and policy support, therefore, depends on a two-way process of access between political members of the executive and officials.

Some of the precise mechanisms for executive control include the following: restrictions on covert action; the formulation of written policies or targets to guide agency priorities; a right to be briefed; the requirement that sensitive matters be approved specifically by ministers; processes of budgetary approval; and regular reporting and audit. In many countries, the minister is often aided in the task of control by an inspector general—an institution most often established by law and endowed with various rights and responsibilities vis-à-vis both the executive and the parliament. In this context, the inspector general monitors

whether the government's intelligence policies are appropriately implemented by the services.

International Cooperation

One area in which it is especially difficult for national ministers (or indeed legislatures) to exercise scrutiny lies within the work of international/supranational bodies and bilateral cooperative arrangements.[34] Bilateral cooperation normally involves sharing intelligence information and analysis on topics of mutual interest.[35] The potential of these arrangements to bypass domestic controls on issues such as surveillance and to impinge on international relations suggests that, nevertheless, there is strong case for legal provisions asserting the need for executive approval. A recent example of legislation addressing this issue comes from Bosnia and Herzegovina: Article 64 of the Intelligence Service Act requires approval to be given before the agency enters into an arrangement with intelligence and security services of other countries. Additionally, the Minister for Foreign Affairs must be consulted before an arrangement is entered with an institution of a foreign state, an international organization of states, or an institution thereof. The Intelligence Committee must also be informed of all such arrangements. It is notable that the Council of Europe has in the context of recent allegations concerning illegal renditions recently argued that parliamentary committees also should assert their power to review the operations of partner agencies within their territory.[36]

Safeguards Against Ministerial Abuse

Alongside powers of executive control there are also various forms of counterbalancing safeguards against political abuse that countries have adopted. In Canada, Hungary, and Australia there is a requirement that certain ministerial instructions be put in writing. Such a stipulation deals with concerns about the executive claiming plausible deniability of certain matters.[37] Ministerial instructions may also be required to be disclosed outside the agency. The Canadian law, for example, requires them to be given to the review body,[38] and Australian law requires them to be given to the Inspector General of Intelligence and Security as soon as practical after the direction is given.[39]

Within a wider frame of checks and balances, the Australian intelligence legislation features another safeguarding provision, namely, the duty of the director-general to brief the leader of the opposition for the purpose of keeping him or her informed on matters related to the agency.[40] Notice that this is also established informal practice in other national settings aiming, inter alia, at the prevention of ministerial abuse. A bipartisan approach to security and intelligence is more likely to be maintained if leading opposition parliamentarians do not feel that they have been wholly excluded from the ring of secrecy. The Australian example operates within a Westminster-style democracy, albeit a federation. In a

more complex federal presidential state, there may be a range of actors who should be briefed on a need-to-know basis, as in Bosnia and Herzegovina.[41]

Legislation from Bosnia and Herzegovina and the United Kingdom, for example, includes clear provisions that the intelligence/security services shall not be amenable to any attempts that try to undermine their impartiality—be it by furthering the interests of certain political parties or by undermining the credibility of legitimate political movements within the country.[42]

Finally, the grant to an agency head of a right of access to the prime minister or president can serve as a safeguard. In the United Kingdom, for example, the agency heads of the Security Service, the Secret Intelligence Service, and the Government Communications Headquarters, although responsible to the Home Secretary and Foreign Secretary, respectively, have a right of access to the prime minister.[43]

THE ROLE OF PARLIAMENT

As a consequence of the democratization of intelligence over the past three decades, in liberal democracies it became common to reserve a role for parliament in the oversight of security and intelligence services. Parliamentary involvement can help ensure that security and intelligence organizations are serving the state as a whole and protecting the constitution, rather than narrower political or sectional interests. There are dangers, however, in parliamentary scrutiny. The security sector may be drawn into party political controversy; an immature approach by parliamentarians may lead to sensationalism in public debate and to wild accusations and conspiracy theories aired under parliamentary privilege. Furthermore, effective scrutiny of security is painstaking and unglamorous work for politicians, conducted almost entirely behind the scenes.

In this section we focus on four important aspects of parliamentary oversight: the mandate of the parliamentary oversight body, members of the oversight body, access to classified information, and budget control.

Mandate of the Parliamentary Oversight Body

The international norm is for parliament to establish an oversight body for all the major security and intelligence agencies (a "functional approach" to oversight), rather than having multiple oversight bodies for specific agencies (an "institutional" approach). This functional approach facilitates seamless oversight because, in reality, different parts of the intelligence machinery work closely with each other. There is a risk that an oversight body established on a purely institutional basis may find that its investigations are hampered if they lead in the direction of information supplied by or to an agency outside the legal range of operation. There are some significant divergences from this approach, however. In the United States, there are separate congressional intelligence committees in

the House of Representatives and the Senate, each with legal oversight of the agencies. In the United Kingdom, the legal responsibilities of the Intelligence and Security Committee (ISC) cover only part of the intelligence establishment (Defence Intelligence Staff, the Joint Intelligence Committee, and National Criminal Intelligence Service are not included within the legal boundaries of the Committee). In practice, however, and with the cooperation of the government, the ISC has examined their work as well.

Broadly speaking, there are two ways in which a parliamentary oversight committee's role can be set out in law. The first is to give a wide range of responsibility and then detail specific matters that may *not* be investigated; examples of this approach can be found in legislation from the United Kingdom and Australia.[44] The second is to write down in the law a comprehensive list of oversight functions of the parliamentary oversight body, for example, as in the United States.[45]

There is a great variety in types of mandate of the parliamentary oversight body. Some oversight bodies have the power to scrutinize the operations of intelligence agencies. For example, both the U.S. congressional oversight committees as well as the Control Panel of the German Bundestag oversee the operations of their respective nation's intelligence agencies.[46] A parliamentary oversight body able to examine intelligence operations may have greater credibility and may be given greater powers (for example, to compel the production of evidence); however, it will face inevitable restrictions on how it conducts its investigations and on what can be reported to parliament or to the public. It will operate in effect within the ring of secrecy, and that will create a barrier between it and the remainder of parliament.

An alternative approach is to limit the function of the parliamentary oversight body to matters of policy, administration, and finance only (as is the case in the United Kingdom). These are issues that can be more readily examined in the public arena with the need for far fewer restrictions in the national interest on what is disclosed. The difficulty of this approach, however, is that it detracts from one of key tasks of parliamentary scrutiny: to ensure that government policy in a given field is carried out effectively. Without access to *some* operational detail, an oversight body can have or give no assurance about the efficiency of the security and intelligence agency in implementing the published policy. The same applies to auditing issues of legality or the agencies' respect for fundamental rights—tasks that are given to parliamentary oversight bodies in some countries, as in Norway.[47] Such exercises in parliamentary oversight may lack credibility unless founded on some clear evidence about the behavior of the agency concerned.

Members of the Parliamentary Oversight Body

To enjoy legitimacy and command trust, it is vital that parliamentary intelligence oversight bodies have a broad mandate, are appointed by Parliament

itself, and represent a cross-section of political parties. Although wherever possible members should have some relevant expertise (say, from previous ministerial service), in our view it is also essential that they be civilian; there must be clear demarcation between the oversight body and the agencies overseen for oversight to be effective. A particular difficulty arises in transition states—the presence of former members of the security agencies on the oversight body. Where the services were implicated in maintaining a repressive former regime, this is bound to undermine confidence in the oversight process and is best avoided, if necessary by a legal prohibition. Equally, to be effective a parliamentary committee must enjoy a relationship of trust with the agencies it oversees. This suggests that to be effective a relatively small committee (without, however, compromising the principle of cross-party membership) is best.

Because the oversight of security and intelligence services requires expertise and time, some parliaments have chosen to set up an outside committee, whose members are not parliamentarians but report to parliament. Examples include the Netherlands, Belgium, Norway, and Canada.[48]

Options for appointing the membership of oversight bodies vary from countries where the head of government appoints (after consultation with the leader of the opposition, in the case of the United Kingdom),[49] to where the executive nominates members but parliament itself appoints (as in Australia),[50] to instances in which the legal responsibility for appointment rests solely with the legislature (as in Argentina,[51] Germany,[52] and Norway).[53]

The chairperson of an oversight body will invariably have an important role in leading it and determining how it conducts its business as well as directing liaison with the services outside formal committee meetings. Traditions within parliamentary systems vary concerning the chairmanship of parliamentary committees. While being sensitive to different traditions, the legitimacy of a parliamentary oversight body will be strengthened if it is chaired by a member of the opposition (as in Hungary),[54] or if the chair rotates between the opposition and the government party. The chairperson should be chosen by parliament or by the committee itself (as in Argentina), rather than appointed by the government (as in the United Kingdom).

Access to Classified Information

The parliament, and particularly the oversight body, needs to have sufficient power to obtain information and documents from the government and intelligence services. The precise extent that a parliamentary oversight body requires access to security and intelligence information and the type of information concerned depends on the specific role that it is asked to play. An oversight body whose functions include reviewing questions of legality, effectiveness, and respect for human rights will require access to more specific information than one whose remit is solely policy. Similarly, it will have a stronger case for a right of access to documents (rather than information or testimony from identified witnesses).

Clearly, however, an oversight body should have unlimited access to the necessary information to discharge its duties, as, for example, in Argentina.[55]

The differences in role explain some of the variations in the extent to which oversight bodies are given access to operational detail in different constitutional systems. Some countries (e.g., the United States) provide that the executive has the legal responsibility to keep the congressional intelligence committees fully and currently informed of the intelligence activities of the United States.[56] Moreover, the U.S. congressional oversight provisions established in 1980 demand that the President keep the two intelligence committees in Congress informed about all covert action operations, including significant failures, before initiation of the covert action authorized by the presidential finding.[57] In the Intelligence Authorization Act of 1991, the President promised to continue to inform Congress in advance in most instances, but he has successfully insisted on flexibility in times of crises—as defined by the White House.[58]

Systems vary in how they handle reporting of sensitive material. In the United States, on the one hand, the onus of being informed rests not only with the oversight body but with the executive as well. In Australia, on the other hand, the parliamentary committee is forbidden from requiring "operationally sensitive information" to be disclosed;[59] requests for documents cannot be made be made by the committee to agency heads, staff members, or the inspector general; and ministers may veto evidence from being given.[60] A power of veto of this kind effectively returns disputes over access to information to the political arena.

Various countries have stipulated that the oversight body is also entitled to obtain information and documents from experts of both the services as well as civil society, for example, think tanks or universities. Such a provision guarantees that parliament is able to receive alternative viewpoints, in addition to the position of the government. For example, in Luxembourg the Parliamentary Control Committee can decide, with two-thirds majority and after having consulted the director of the Intelligence Services, to be assisted by an expert.[61] If parliament lacks clear information or doubts the validity of government information, legislators may have the power to start their own inquiry, for example, in Argentina, Norway, South Africa, South Korea, United Kingdom, and the United States. Of these selected states, the legislative oversight bodies of Norway, South Africa, and the United States possess subpoena powers.[62]

However, because the information and documents are often related to sensitive issues (about persons) and/or about national security, oversight bodies of various countries have made great efforts to protect information from unauthorized disclosure. Unauthorized disclosure of information may harm not only national security interests but also the trust that is necessary for an effective relationship between the oversight body and the services. This is partly a matter of legislation (see the United States and Norway),[63] and partly a matter of proper behavior of the members of the oversight body in dealing with classified information with care and attention.

Parliamentary Budget Control

Budget control is at the heart of parliamentary control. Most countries have developed or are developing a systematic approach to the evaluation and approval of budget proposals. In every country, parliament fulfills a different role in the budgeting and accounting procedures for the security and intelligence services, for example, in terms of the scope of budget control, the power to amend budgets, the power to approve supplementary budget requests, access to classified information, and the disposition of independent financial auditors. The greater the parliament's powers in these areas, the more effective it will be in debates with the government.

Budget control has to be understood in the context of the mandate of the parliamentary intelligence oversight body. In some countries, this body clearly has the power of the purse as the embodiment of the people's voice. In other countries, for example in Norway, parliament has chosen not to give the power of the purse to the oversight committee but to keep it for the plenary or parliamentary budget committee. The reason behind this practice is that budget control would make the oversight committee co-responsible for government policy.

In other parliaments, however, such as in Argentina, the Netherlands, Germany, or the United States, the parliamentary oversight committee has the power of the purse, giving those legislatures control over how money is spent by the services. To be more precise, in the United States as well as, for example, Germany, budgetary power is often divided between the budget committee and the intelligence oversight committee. The former committee focuses on appropriations; the latter focuses on the policy aspects of the services and authorizes funds. Some governments also keep parliament informed about the execution of the intelligence budget during the fiscal year (as in Germany).[64] The state budget concerning the different aspects of the security sector has to be all-inclusive and complete. No expenditure should go unaccounted for. "Black" programs or secret budgets—inaccessible for members of the parliamentary intelligence oversight committee—would be clearly in violation of this principle. Parliamentarians of the intelligence oversight committee and the budget committee should have access to all classified information, as is the case in Hungary.[65]

INDEPENDENT COMPLAINTS, INSPECTION, AND AUDIT PROCESSES

Our third category of oversight structures embraces a variety of concerns, from authorizing the use of special powers, to dealing with complaints brought by citizens, to checking that the services have used their powers with propriety and with financial regularity. What these disparate concerns have in common is that various countries have found it useful to involve politically independent officials

and institutions, mostly in ex post facto review, but occasionally in the prior authorization of the work of the agencies.

In other areas of government, this is a task that one would expect to find the judiciary discharging as the third branch, alongside the executive and the legislature. That, however, is rarely appropriate or effective in matters touching national security.[66] Occasionally legal regimes have been constructed that under highly quarantined circumstances involve judges in authorizing or affirming actions based on intelligence, as with the Foreign Intelligence Surveillance Act in the United States, the equivalent role of the Federal Court in Canada, or control orders under the Terrorism Act of 2005 in the United Kingdom. However, the secret nature of the processes involved, difficulties in obtaining evidence, and the legitimate need of these agencies to protect sensitive information from public disclosure can all be cited as objections to adjudication through public hearings in the regular courts.

Nevertheless, there is a clear need for some avenue of redress for individuals who claim to have been adversely affected by the exceptional powers, such as surveillance or security clearance, often wielded by security and intelligence agencies. Complaints may have a broader role to play also in highlighting administrative failings and lessons to be learned, leading to improved performance. Clearly, however, any system for redress needs to be designed to prevent legitimate targets of a security or intelligence agency from finding out about the agency's work. Achieving this balance in a complaints system between independence, robustness, and fairness, on one hand, and sensitivity to security needs, on the other hand, is challenging but not impossible. The requirements of human rights treaties, and especially for European states the European Convention on Human Rights, with its attendant protection of fair trial, respect for private life, and the requirement of an effective remedy, also have a considerable bearing on these matters, but these detailed technical questions cannot be pursued here.[67]

Different oversight systems handle complaints in a variety of ways. An independent official, such as an ombudsman, may have power to investigate and report on a complaint against an agency. This is the case in the Netherlands.[68] In some countries an independent inspector-general of security and intelligence deals in a rather similar way with complaints against the services as part of the office's overall oversight duties. This is the case, for example, in New Zealand (Office of Inspector-General of Intelligence and Security, established in 1996) and South Africa (Office of Inspector General of Intelligence, appointed pursuant to section 12 of the Constitution). In addition, specific offices established under freedom of information or data protection legislation may have a role in investigating complaints against the agencies.

Ombudsman-type systems place reliance on an independent official investigating on behalf of the complainant. They usually exist to deal with an administrative failure rather than a legal error as such. They give less emphasis to the complainant's own participation in the process and to transparency. They typically conclude with a report, and (if the complaint is upheld) a recommendation

for putting matters right and future action, rather than a judgment and formal remedies.

Less commonly, complaints and grievances of citizens are may be dealt with by the parliamentary intelligence oversight committee, as is the case, for example, in Germany and Norway.[69] On the one hand, there may be a benefit for a parliamentary oversight body in handling complaints brought against security and intelligence agencies since this will give an insight into potential failures—of policy, legality, and efficiency. On the other hand, if the oversight body is too closely identified with the agencies it oversees or operates within the ring of secrecy, the complainant may feel that the complaints process is insufficiently independent. In cases where a single body handles complaints and oversight, it is best if there are quite distinct legal procedures for these different roles. Generally, it is preferable that the two functions be given to different bodies, but that processes are in place so that the oversight body is made aware of the broader implications of individual complaints.

In some countries not only citizens but also members of the services are permitted to bring service-related issues to the attention of an ombudsman or parliamentary oversight body. For example, in Germany officials may raise issues with the Parliamentary Control Panel,[70] and in South Africa members of the service may complain to the inspector general.

Another method of handling complaints is through a specialist tribunal. This may be established to deal with complaints either against a particular agency or in relation to the use of specific powers, as in the United Kingdom (the Intelligence Services Commissioner and the Commissioner for the Interception of Communications). Or complaints may be handled in a tribunal-type procedure but by a specialist oversight body, as with the Security Intelligence Review Committee (SIRC) in Canada. On the one hand, a tribunal of this kind has some advantages over a regular court in dealing with security- and intelligence-related complaints: it can develop a distinct expertise in the field of security and intelligence, devised for handling sensitive information. In view of the nature of the subject matter, these are unlikely to involve a full public legal hearing. On the other hand, although some tribunals may give the complainant a hearing, he or she is likely to face severe practical difficulties in proving a case, in obtaining access to relevant evidence, or in challenging the agency's version of events. To combat some of these problems special security-cleared counsels have been introduced in Canada and the United Kingdom. These counsels have the task of challenging security-related arguments, especially those aspects not disclosed to the complainant. This can help the tribunal reach a more objective assessment of the evidence and the arguments.

Apart from redress of complaints, a second reason for the creation of independent offices is to provide impartial verification and assurance for the government that secret agencies are acting according to its policies effectively and with propriety. For this reason, a number of countries have devised offices such as inspectors-general, judicial commissioners, or auditors to check on the activities

of the security sector and with statutory powers of access to information and staff.[71]

This notion derives from the U.S. intelligence community, which now has around a dozen inspectors general. All are independent of the agencies concerned. There are, however, significant variations among them: some are established by legislation (for example, the inspectors general for the Central Intelligence Agency and the Department of Defense); others are the creatures of administrative arrangements established by the relevant secretary (for example, with regard to the Defense Intelligence Agency and the National Reconnaissance Office, both located within the organizational framework of the Department of Defense). Irrespective of this distinction, some report to Congress as well as to the executive branch. A number of these offices have a responsibility that extends to efficiency, avoiding waste and audit, as well monitoring legality and policy compliance.

A common feature is that inspectors general operate within the ring of secrecy: their function is not primarily to provide public assurance about accountability, rather to strengthen accountability to the executive. The Canadian inspector general is a clear illustration of this type of office and is entrusted with unrestricted access to information in the hands of the Service to fulfill these functions.[72] Likewise in Bosnia and Herzegovina, the inspector general exercises "an internal control function."[73] To this end, the inspector general may review intelligence activities; investigate complaints; initiate inspections, audits, and investigations on his or her own initiative; and issue recommendations. The inspector general has a duty to report at least every six months to the Security Intelligence Committee and keep the main executive actors informed of developments in a regular and timely fashion. The powers of the inspector general include questioning agency employees and obtaining access to agency premises and data.

In other countries—notably South Africa—the role is different, that is, to report to parliament. In effect the office bridges the ring of secrecy: it is an attempt to assure the public through a report to parliament that an independent person with access to the relevant material has examined the activities of the security or intelligence agency. However, inevitably most of the material on which an assessment of the agency's work is made has to remain within the ring of secrecy, although it may be shared with other oversight bodies.

Even some inspectors general whose statutory brief is to report to the executive may maintain an informal working relationship with parliamentary bodies. This is so in Australia for instance, and as noted, a number of the U.S. inspectors general report periodically to Congress.

Whether an office of this kind reports to the government or to parliament, in either case, careful legal delineation of its jurisdiction, independence, and powers are vital. Independent officials may be asked to review an agency's performance against one or more of several standards: efficiency, compliance with government policies or targets, propriety, or legality. In any instance, however, the

office will need unrestricted access to files and personnel to be able to come to a reliable assessment. In practice an independent official is unlikely to be able to scrutinize more than a fraction of the work of an agency. Some of these offices work by sampling the work and files of the agencies overseen; this gives an incentive for the agency to establish more widespread procedures and produces a ripple effect. Some also have jurisdiction to deal with individual complaints, as under the Australian scheme.[74]

A third independent review function concerns financial propriety. Both the executive and the legislature have a legitimate interest in ensuring that budgets voted for intelligence are spent lawfully and effectively. However, as with the handling of complaints, it requires some ingenuity to devise systems for protecting secrecy while nevertheless ensuring that auditors have the wide access to classified information necessary to certify whether the services have used government funds within the law. Understandably, limited restrictions to protect the identities of certain sources of information and the details of particularly sensitive operations may be imposed on the access granted to an auditor general.[75]

Primarily what distinguishes the auditing security and intelligence services from regular audits of other public bodies, however, are the reporting mechanisms. To protect the continuity of operations, methods, and sources of the services, special reporting procedures are in place in many countries. For example, in the United Kingdom only the chairs of the Public Accounts Committee and the Intelligence and Security Committee are fully briefed about the outcome of the financial audit. These briefings may include reports on the legality and efficiency of expenditures, occurrence of possible irregularities, and whether the services have operated within or have exceeded the budget. In many countries, the public annual reports of the security and intelligence service (as in the Netherlands) or of the parliamentary oversight body (as in the United Kingdom) include statements about the outcome of the financial audits.[76]

CONCLUSION

In this chapter we have compared the principles, laws, and mechanisms of national intelligence oversight in various democracies; both in old democracies (e.g., the United Kingdom and the Netherlands) as well as in new democracies (e.g., Hungary and South Africa). The purpose was not so much to give a representative overview of intelligence oversight in democracies but to identify approaches that various states have adopted to support democracy, the rule of law, and human rights in this field. A comprehensive approach to accountability was used, which included four layers of accountability: internal control within the agency, the executive, parliament, and independent review bodies such as the ombudsman and national audit offices.

As mentioned in the introduction, intelligence oversight is a very recent development, which started about thirty years ago in liberal democracies. It is not

surprising, therefore, that most of the examples we have discussed are based on laws enacted in the late 1980s and the beginning of the 1990s.

The first point to make is that national security is not only a powerful argument against democratic oversight in dictatorial or one-party states but also, until recently, in established democracies such as the United Kingdom and the United States, where oversight legislation was adopted in 1989 and 1974, respectively. According to this argument, national security requires that full secrecy be observed and that the services can be only accountable to a small group of decision makers. This argument, however, goes contrary to the very nature of a democratic polity, which is that all issues vital to the lives of its citizens should be subject to normal democratic decision-making procedures. The mechanisms of intelligence accountability identified and analyzed in this chapter do show clearly that the arguments of national security and democracy can be reconciled. Accountability procedures such as reporting illegal activities within the agency, the practice of consulting the leaders of both opposition and government parties in the appointment of the agency director, access of members of parliament to classified information, independent financial audit as well as ministerial procedures for approving covert action and international intelligence sharing—all show that democratic decision and serious program review can be applied to the area of intelligence. The fear that involving parliament and, above all, members of the opposition would lead to intelligence leaks, seems to be largely unfounded. On the contrary, for example, the recent reports of intelligence leaks in the United States show that not members of the Congress but mostly members of the intelligence agencies and the executive, up to the level of the President, have leaked classified information to the press.

The second point is related to the question of whether these rather young accountability provisions and practices are strong enough to withstand major challenges to intelligence oversight. In particular after 9/11, new developments have challenged and tested the robustness of national intelligence oversight systems. We list some of these problems here. A first issue is the problem of gearing national oversight institutions toward the oversight of *international* intelligence cooperation. This problem is aggravated by the lack of democratic oversight of intelligence on the international level. A second problem is the oversight of the greater powers that governments acquired after 9/11 for dealing with terror (e.g., the new 2004 Civil Contingencies Bill in the United Kingdom and the 2001 USA-PATRIOT Act in the United States). A third danger is the politicization of the services, which refers to the use of intelligence services for personal or political party purposes in both new and old democracies.

The danger of politicization of the intelligence services is the downside of the increasing democratization of intelligence oversight. On one hand, greater transparency and public accountability leads to a better checks and balances of the services. On the other hand, the services and their activities are increasingly becoming part of the normal political debate, which leads to the danger that

actors in that political debate will use the services and their work for their own parochial interests.

Whether the systems of checks and balances are strong enough to ensure a proper and lawful control of the services eventually will be known. This brings us to the last and third point. It is important to note that the intelligence agency is included in the framework of the four layers of accountability. The agency, properly understood, is itself not just an object for control.

NOTES

1. Hans Born, Loch Johnson, and Ian Leigh, eds., *Who's Watching the Spies? Establishing Intelligence Service Accountability* (Dulles, VA: Potomac Books, 2005); Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005); Jean-Paul Brodeur, Peter Gill, and Dennis Töllborg, *Democracy, Law and Security: Internal Security Services in Contemporary Europe* (Aldershot: Ashgate, 2003); Laurence Lustgarten and Ian Leigh, *In from the Cold: National Security and Parliamentary Democracy* (Oxford: Clarendon Press, 1994).

2. Concerning the United States, see U.S. Senate, *Final Report,* Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee), 94th Congress, 2nd sess., Rept. 94-755 (May 1976); Loch K. Johnson, *A Season of Inquiry* (Lexington: University Press of Kentucky, 1985).

3. Respectively, Government of Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Second Report, *Freedom and Security Under the Law*, 2 vols. (Hull: Ministry of Supply and Services Canada, August 1981) [the McDonald Commission report]; Royal Commission on Intelligence and Security, *Fourth Report* (Canberra, 1977) [the Hope report]; Dok. no. 15 (1995–96) [the Lund report].

4. It has to be noted, however, that parliamentary oversight of the intelligence services was in place in the Netherlands and Germany since 1952 and 1956, respectively.

5. Recommendations 1402/1999 and 1713/2005 of the Council of Europe Parliamentary Assembly; Western European Union Assembly Resolution 113, adopted on December 4, 2002 (9th sitting).

6. Law on the Intelligence and Security Agency of Bosnia and Herzegovina, passed in March 2004. Slovenia: Law on Defense (December 28, 1994), arts. 33–36; The Basics of National Security of Lithuania (1996); Estonia: Security Authorities Act, passed December 20, 2000; RSA, Intelligence Services Act (1994) (as amended).

7. Kevin O'Brien, "Controlling the Hydra: A Historical Analysis of South African Intelligence Accountability," in Born, Johnson, and Leigh, *Who's Watching the Spies?*

8. Eduardo Estevez, "Argentina's New Century Challenge: Overseeing the Intelligence System," in Born, Johnson, and Leigh, *Who's Watching the Spies?*

9. Jonathan Moran, "The Role of Security Services in Democratization: South Korea's Agency for National Security Planning," in Born, Johnson, and Leigh, *Who's Watching the Spies?*

10. Iain Cameron, *National Security and the European Convention on Human Rights* (Uppsala: Lustu Forlag, 2000); Iain Cameron, "Beyond the Nation State: The Influence of the European Court of Human Rights on Intelligence Accountability," in Born, Johnson, and Leigh, *Who's Watching the Spies?*

11. *Harman and Hewitt v. UK* (1992) 14 EHRR 657; *V and Others v. Netherlands*, Commission report of December 3, 1991; *Rotaru v. Rumania,* Appl. No. 8341/95, May 4, 2000.

12. Law on the Intelligence and Security Agency, Bosnia and Herzegovina (2004), art. 5.

13. National Intelligence Law no. 25520, Argentina (2001), art. 4.

14. Act Governing the Supervision of the Police and Intelligence Services (1991), art. 17.

15. Intelligence Service Act, Australia (2001) (Cth), part 3, section 17 (3).

16. Hungarian Law on the National Security Services, Act 125 (1995), section 11.2.

17. The Internal Security Agency and Foreign Intelligence Act, Poland (2002), art. 16.

18. Further information is available at http://www.pentagon.mil/atsdio/mission.html.

19. Law on Intelligence and Security Agency, Bosnia and Herzegovina (2004), art. 14.

20. Hungarian Law on the National Security Services, Act 125 (1995), section 27.

21. Section 15.5 of the Canadian Security of Information Act (2003).

22. Further information available at http://www.pentagon.mil/atsdio/faq.html.

23. Republic of South Africa, *White Paper on Intelligence* (1994), annex A.

24. Richard Best, *Intelligence Issues for Congress* (Washington, DC: Congressional Research Service, 2001).

25. Commission of Enquiry into Certain Actions of the RCMP, *Freedom and Security under the Law* (Ottawa, 1980), vol. 1, pp. 513ff.

26. German Sicherheitsüberprüfungsgesetz (1994); Dutch Intelligence and Security Services Act (2002); U.K. Regulation of Investigatory Powers Act (2000).

27. German Bundesverfassungsschutzgesetz (1990), §9(3) 2.

28. Lustgarten and Leigh, *In from the Cold*, chap. 15.

29. Canadian Security Intelligence Service Act 1984, s. 13

30. Peter Gill, "The Politicization of Intelligence: Lessons from the Invasion of Iraq," in Born, Johnson, and Leigh, *Who's Watching the Spies?*

31. Intelligence Services Act, Canada, R.S. (1985), emphasis added.

32. Internal Security Agency and Foreign Intelligence Agency Act (2002), Poland, art. 7.

33. Law on the Intelligence and Security Agency (2004), Bosnia and Herzegovina, arts. 8 and 9.

34. Note, for example, Art. 85 of the Constitution of Bulgaria, which requires parliamentary approval for treaties with military or political implications.

35. Jeffrey T. Richelson and Desmond Ball, *The Ties That Bind* (London: Allen & Unwin, 1990).

36. "Secretary General's report under Article 52 ECHR on the question of secret detention and transport of detainees suspected of terrorist acts, notably by or at the instigation of foreign agencies," *Council of Europe*, SG/Inf (2006) 5, Strasbourg, pnt. 101, available at http://www.coe.int/T/E/Com/Files/Events/2006-cia.

37. Canadian Security Intelligence Service (CSIS) Act (1984), sections 7(1) and (2); Act on the National Security Services (1995), Hungary, section 11.

38. CSIS Act, s. 6(2).

39. Australian Inspector-General of Intelligence and Security Act (1986), section 32B.

40. Intelligence Services Act, Australia (2001), section 19.

41. Law on the Intelligence and Security Agency, Bosnia-Herzegovina (2004), art. 6.

42. Law on the Intelligence and Security Agency (2004), Bosnia and Herzegovina, art. 39. In the United Kingdom see Security Service Act (1989), s. 2(2)(a); Intelligence Service Act (1994), s. 2(2)(b), 4(2)(b).

43. Security Service Act (1989), s. 2(4); Intelligence Service Act (1994), s. 2(4), 4(4).

44. Concerning Australia: Intelligence Services Act. No. 152 (2001), sections 28 and 29. Concerning the United Kingdom: Intelligence Services Act (1994), s. 10.

45. Section 13, U.S. Rules of the U.S. Senate Select Committee on Intelligence.

46. German Bundestag, Secretariat of the Parliamentary Control Commission, *Parliamentary Control of the Intelligence Services in Germany* (Berlin: Bundespresseamt, 2001)

47. The Act Relating to the Monitoring of Intelligence, Surveillance and Security Services, Act no. 7 (February 3, 1995_, Norway

48. Until 2004 there was no oversight committee in the Canadian Parliament, although the Security Intelligence Review Committee (a statutory body composed of Privy Counsellors) was established under the Canadian Security Intelligence Service Act (1984). A parliamentary oversight committee is soon to be established.

49. Intelligence Services Act (1994), s. 10.

50. Intelligence Services Act (2001), s. 14(2).

51. Estevez, "Argentina's New Century Challenge," in Born, Johnson, and Leigh, *Who's Watching the Spies?*

52. Law on the Parliamentary Control of Activities of the Federal Intelligence Services (PKGrG) (1978; 1992, 1999, and 2001 amended version).

53. Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS) (1995), section 1.

54. Section 14, 1, Act no. 125 (1995) on the National Security Services, Hungary.

55. Art. 32, National Intelligence Law, no. 25520, Argentina (2001).

56. U.S. Code, Title 50, Section 413 (a).

57. U.S. Code, Title 50, Section 413.

58. Loch K. Johnson, "Governing in the Absence of Angels: On the Practice of Intelligence Accountability in the United States," in Born, Johnson, and Leigh, *Who's Watching the Spies?*, pp. 64–65.

59. Intelligence Services Act (2001), s. 30 (Australia).

60. Ibid., s. 32.

61. Art. 14 (4), Loi du 15 Juin portant organisation du Service de Renseignement de l'Etat, Memorial-Journal Officiel du Grand-Duché de Luxembourg (2004), A-No. 113.

62. Hans Born, "Balancing Operational Efficiency and Democratic Legitimacy," in Born, Johnson, and Leigh, *Who's Watching the Spies?*, pp. 230 and 237.

63. U.S. Code Section 413, General Congressional Oversight Provisions, (d); The Act Relating to the Monitoring of Intelligence, Surveillance and Security Services (1995), Section 9, (Norway).

64. German Bundestag, Secretariat of the Parliamentary Control Commission (PKGr), *Parliamentary Control of the Intelligence Services in Germany* (July 2001).

65. Article 14, 4g, of the 1995 Act on the National Security Services of Hungary.

66. Lustgarten and Leigh, *In from the Cold*, chap. 12.

67. *Klass v. Germany*, para. 15 (regarding Art. 8); *Leander v. Sweden*, para. 68 (regarding Art. 13). See Cameron, *National Security and the European Convention on Human Rights*; Cameron, "Beyond the Nation State."

68. Intelligence and Security Services Act (2002), art. 83.

69. Fredrik Sejersted, "Intelligence and Accountability in a State Without Enemies," in Born, Johnson, and Leigh, *Who's Watching the Spies?*

70. German Bundestag Secretariat of the Parliamentary Control Commission (PKGR), *Parliamentary Control of the Intelligence Services in Germany* (Berlin: Bundespresseamt, 2001), pp. 19–20.

71. For comparison of the powers of inspectors general in different countries, see Intelligence and Security Committee (U.K.), *Annual Report for 2001–2*, Cm 5542, Appendix 3.

72. CSIS Act, 1984, s. 33.2 and 33.3.

73. Law of the Intelligence and Security Agency of Bosnia Herzegovina, art. 32.

74. Inspector-General of Security and Intelligence Act (1986), sections 10–12.

75. These restrictions apply to the U.K. comptroller and auditor general, see Report by the Comptroller and Auditor-General, *Thames House and Vauxhall Cross,* HC Session 1999–2000 (February 18, 2000), point 8, available at http://www.nao.org.uk/publications/nao_reports/9900236.pdf.

76. See, for example, Annual Report of the General Security and Intelligence Services of the Netherlands (2003), available at http://www.minbzk.nl/contents/pages/9459/annual_report_2003_aivd.pdf, pp. 69–70; UK Parliamentary Intelligence and Security Committee Annual Report 2002–2003, presented to Parliament by the Prime Minister by Command of Her Majesty (June 2003), London, pp. 8–13.

8

THE COIN OF INTELLIGENCE ACCOUNTABILITY

A. DENIS CLIFT

THE SETTING

TO PROVIDE A GOVERNMENT OF THE PEOPLE, by the people, for the people, the Constitution of the United States created three separate branches—executive, legislative, and judicial—to exercise the government's lawful powers. By design, each of the three independent branches was given checks and balances against the others. Accountability—the imperative of each individual of government and each organization of government being liable to answer for exercise of duties, responsibilities, and conduct—was at the heart of these checks and balances.

The roles played by print and electronic media and by citizens and private organizations both augment and subdue the role of government, variously sounding alarm and sounding praise, calling for inquiry and challenging any such call. In this era of globalization, this cyber era, this information age, international political, economic, cultural, religious, health, environmental, and security issues must be weighed in the exercise of the government's powers.

If it is the people's government, the people have a right to know. Where the work of intelligence is secret, because it is seeking information that is being hidden, withheld, or denied by foreign sources—or because it is operating covertly to hide U.S. involvement—that secrecy conflicts with the right to know. The work of intelligence must be accountable. The early twenty-first century finds the checks and balances of the American system being applied with broad reach and great depth to the work of U.S. intelligence, which is accorded an importance higher than ever in the work of the nation. Intelligence performs its responsibilities as a member of the executive branch, with the intrusive oversight of the

legislative and judicial branches, with periodic examinations by commissions, and under the eyes of the media and the public.

In terms of positive responsibilities, intelligence is held accountable for delivering the highest quality warnings, assessments, analysis, and actions contributing to the effective safeguarding of America and the advancement of U.S. interests. On the reverse side of this coin, intelligence is held strictly accountable for acting within the law and in keeping with the principles of the American democracy, respecting the rights and liberties of U.S. citizens.

The first play of intelligence in U.S. history dates back to the American Revolution. George Washington operated intelligence networks against the British and believed deeply in their value. In a letter to one of his colonels in 1777, he counseled: "The necessity of procuring good intelligence is apparent & need not be furthered urged—All that remains for me to add is, that you keep the whole matter as secret as possible. For upon Secrecy, Success depends in most Enterprizes of the kind, and for want of it, they are generally defeated, however well planned & promising a favorable issue."[1]

Although intelligence figured prominently in the Civil War, for most of the nation's early life, it figured almost not at all. The vast, shielding expanses of the Atlantic and Pacific Oceans were the only protective deterrents needed while the young nation was coming of age. From the late nineteenth century until World War II, U.S. intelligence operated primarily in the separate preserves of the Navy and Army, with small, separate components in the Department of State, Treasury, and Justice, all well shielded from the public eye.

The emergence and rise of importance of intelligence as an instrument of national power dates back no further than the mid-twentieth century. Formal national structures and processes for holding intelligence accountable emerged in the mid-1970s. Throughout the history of U.S. intelligence until the twenty-first century, where there was accountability, it was in the oversight, watchdog role. From the time of the 1878 Posse Comitatus Act, which prohibited the armed forces from engaging in domestic law enforcement unless specifically authorized, it was held in parallel that U.S. intelligence should not operate against U.S. citizens. In a broader sense, to the degree that there was a public awareness of intelligence operations, it was accompanied by skepticism and distrust. In parallel, in American colleges and universities, academic research on intelligence (to the extent there was such research) and teaching on intelligence tended to adopt the oversight, watchdog role focusing on the negative side of accountability.

General of the Army Dwight D. Eisenhower noted the phenomenon of American distrust in his reflections on the challenges the Army and the nation faced at the dawn of World War II. "The American public," he wrote, "has always viewed with repugnance everything that smacks of the spy; during the years between the two world wars no funds were provided with which to establish the basic requirement of an intelligence system—a far-flung organization of factfinders."[2]

Eisenhower's deputy in the 1943 North African campaign, Maj. Gen. Omar Bradley, agreed. Describing the situation at the U.S.-British Allied Force

Headquarters in Algiers, he observed, "In their intelligence activities at [Headquarters], the British easily outstripped their American colleagues. The tedious years of pre-war study the British had devoted to areas throughout the world gave them a vast advantage which we never overcame. The American Army's long neglect of intelligence training was soon reflected in the ineptness of our initial undertakings."[3]

To help meet World War II intelligence needs, President Franklin D. Roosevelt created the first national civilian U.S. intelligence player in the form of the Coordinator of Information. The Office of Strategic Services (OSS) followed and grew to more than 30,000 strong before being disbanded by President Harry S Truman at the end of the war. One passionate OSS veteran wrote: "President Truman, with complete lack of sophistication, reacted as if espionage were something one shouldn't speak about, like syphilis in the family."[4]

In fact, with the passage of the National Security Act of 1947, signed into law by Truman, the Central Intelligence Agency (CIA) was created and declared a formal arrow, together with defense and foreign policy, in the quiver of American security. The act was born out of the nation's determination never again to have failure of warning as experienced at Pearl Harbor. It was legislation passed at the dawn of the nuclear era creating a National Security Council—with the President, Vice President, Secretary of State, and Secretary of Defense as statutory members—and with the CIA responsible to the Council, a CIA to be headed by a Director of Central Intelligence to be appointed by the President with the consent of the Senate.

The act provided for the intelligence work and responsibilities of the separate military departments and other governmental organizations. Within the framework of the act, new intelligence organizations—for example, the National Security Agency in 1952 and the Defense Intelligence Agency in 1961—joined what has become known as the U.S. intelligence community. The nation, now in a Cold War with the Soviet Union, had a daunting nuclear adversary. Successive Directors of Central Intelligence and intelligence community leaders worked relatively smoothly with Congress in the annual intelligence budget requests, which were acted on, by and large, in the late 1940s, 1950s, and 1960s in a minimally intrusive manner.

In the 1970s, newspaper revelations of intelligence community covert actions and alleged wrongdoings—some against U.S. citizens—coming at the time of national and international turmoil over the conflict in Vietnam and the Watergate scandal, caused Congress to impose itself more firmly. Legislation was passed requiring coordination with Congress on covert actions. Lengthy hearings were held, resulting in the creation of standing Senate and House intelligence committees.[5]

For the balance of the century, the committees shifted and reshifted their oversight priorities as they sought to ensure capable U.S. intelligence while guarding against intelligence excesses and wrongdoings. If there was a constancy to their charge under the Constitution, it could be found succinctly in the words of Senator David Boren (D-OK), chair of the Senate Select Committee on

Intelligence from 1987–93, at the outset of the 1987 confirmation hearings of Judge William H. Webster to be Director of Central Intelligence:

> This Committee and the Senate have a duty to the American people to ensure that the new Director of Central Intelligence will conduct a program of effective intelligence gathering within the framework of our laws and our democratic institutions. It is imperative that the Director of Central Intelligence be a person of exceptional ability and integrity, capable of exercising the independence necessary to protect against possible misuse of the Agency and its resources.[6]

At the same time Boren's words captured the role of the Senate and congressional oversight, they underscored the continuing, dominating puritanism in the nation's late 20th-century approach to intelligence, a quality addressed by British author John Ranelagh. "Intelligence is seen as fun by the British (who in the days of empire called it the 'Great Game')," he wrote, "and without morality. Americans see it as having moral importance, and face real crises of conscience when they find they may have to be involved in immoral activity. In America, power is associated with publicity. In Britain (indeed in Europe), power is associated with secrecy."[7]

When terrorists seized U.S. airliners on September 11, 2001, and crashed them into the twin towers of the World Trade Center, the Pentagon, and a field in Pennsylvania, the history of U.S. intelligence turned to a new chapter. On September 20, 2001, President George W. Bush told a joint session of Congress that an act of war had been committed against the United States and that in a single day a different world had emerged with freedom under attack.[8] Only six weeks later, on October 24, 2001, the Congress passed the USA-PATRIOT Act, signed into law two days later, expanding the government's counterterrorist surveillance powers and expanding cooperation between U.S. foreign intelligence and domestic law enforcement. People across the nation were deeply alarmed. The homeland was vulnerable, without deterrent, to a new form of devastating attack. The cry of "intelligence failure" arose across the land. The search for accountability was mounted.

The National Commission on Terrorist Attacks upon the United States, or the 9/11 Commission, and the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, or WMD Commission, were formed. Congressional hearings were held. Reform legislation was drafted, and on January 20, 2004, the Intelligence Reform and Terrorism Prevention Act was passed. The act, 235 pages in length, established a new Director of National Intelligence, legislated reorganization and improvement of management of the intelligence community, assigned specific responsibilities for analytic integrity, established a National Counterterrorism Center, a National Counteproliferation Center, and a Privacy and Civil Liberties Oversight Board, among its key provisions.[9]

The act gave expanded intelligence responsibilities to the Federal Bureau of Investigation (FBI) and not only mandated the sharing of information between

foreign intelligence and domestic law enforcement agencies at the federal level but also directed the flow of information—down and up—among federal, state, local, and tribal authorities. From the work of the commissions, Congress, and the executive branch, a new concept had emerged and was being enacted—the concept of national intelligence.

In October 2005, in his foreword to *The National Intelligence Strategy of the United States of America*, the first Director of National Intelligence John D. Negroponte underlined the need for a fresh, risk-taking strategy for the intelligence challenges of the twenty-first century and the joining of domestic and foreign intelligence into national intelligence. This new approach, he wrote, did not reflect any change to the nation's commitment to civil liberties and freedom.[10] Accountability would remain clearly engraved on both sides of the Republic's intelligence coin of reform.

THE LAW, THE COURTS, THE WHITE HOUSE

George Washington used intelligence extensively in the American Revolution. As the nation's first President, he requested and received authority from Congress for a Contingency Fund for the Conduct of Foreign Intercourse, placed in the budget of the Department of State, to be available for intelligence purposes. In the years that followed, U.S. Presidents rejected requests from Congress for an accounting of expenditures from the fund. In the 1840s, President James Polk turned down such a request, responding in part: "The experience of every nation on earth has demonstrated that emergencies may arise in which it becomes necessary for the public safety or the public good to make expenditures, the very subject of which would be defeated by publicity. In no nation is the application of such funds to be made public."[11]

Though the National Security Act of 1947 established the Senate's advice and consent role in the appointment of the Director of Central Intelligence, the act prescribed no new legislative oversight structure or process for the work of intelligence. In both the Senate and the House, the Armed Services Committee and the Appropriations Defense Subcommittee became the points of oversight for intelligence. Intelligence budgets would be submitted annually and acted on with few questions asked. From the late 1940s through the 1950s and 1960s, the intelligence community went about its work with few hearings and modest intrusion by the legislative branch. Senator Leverett Saltonstall (R-MA) captured the tone of the relationship in a 1956 comment: "It is not a question of reluctance on the part of CIA officials to speak to us. Instead, it is a question of our reluctance, if you will, to seek information and knowledge on subjects which I personally, as a member of Congress and as a citizen, would rather not have."[12]

In the mid-1970s, news reports and other charges spawned a whirlwind of alleged CIA assassination plots, questionable covert actions, and surveillance of American college students and domestic dissenters. There were allegations

of excesses and wrongdoing by other members of the intelligence community, together with allegations of excesses by the FBI, to include charges that the Bureau had acted to discredit the Reverend Martin Luther King Jr. The era of executive-legislative intelligence laissez-faire had passed. The intelligence community would be held to account.

In 1974, Congress passed the Hughes-Ryan Amendment to the Foreign Assistance Act of 1961 requiring the President to review proposed CIA covert actions, to determine—or find—that each such action was in the nation's interest and to submit such findings to six committees of Congress.[13] In 1975, both bodies of Congress established committees to investigate the alleged wrongdoings. The Senate's Select Committee to Study Government Operations with Respect to Intelligence Activities was chaired by Senator Frank Church (D-ID), and was known as the Church Committee. The House's Select Committee on Intelligence, with its second chairman Representative Otis Pike (D-NY), was known as the Pike Committee.

The Church Committee's investigation ran for sixteen months, with the cross-examination of hundreds of witnesses producing thousands of pages of sworn testimony. Several volumes of reports were published, and ninety-six proposals for reform were recommended.[14] The Pike Committee's more sensational report was leaked to the press before publication. This was a tumultuous period, with sensational headlines and sparks flying between the legislative and executive branches. Serving at the time as a senior member of President Gerald R. Ford's National Security Council staff, I can recall in particular the extraordinary rudeness of the Pike Committee staff members I had to deal with. They reminded me of cast members from the film *Lord of the Flies.*

As a result of these investigations, the Senate created the Senate Select Committee on Intelligence in 1976, and the House created the House Permanent Select Committee on Intelligence in 1977. A year later with the passage of the 1978 Intelligence Authorization Act, each committee was given oversight of the intelligence community's budget. Reins of accountability were in the Congress's hands.

• • •

In parallel in 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA), creating the U.S. Foreign Intelligence Surveillance Court in the judicial branch to oversee FBI requests for authority to conduct surveillance against suspected foreign intelligence agents in the United States. Wiretaps would not be permitted unless authorized. This was a very sensitive business. The law provided that the work of the court and its findings would not be available to the public. To provide for situations where a law enforcement agency's request for a surveillance warrant was denied by the court, the Surveillance Act also created a U.S. Intelligence Surveillance Court of Review.

The judicial branch role played by the FISA Court increased significantly both in scope and the volume of court actions after the 2001 terrorist attacks. The

number of FBI requests for surveillance warrants rose, as the Bureau drew on its increased counterterrorist surveillance authorities under the USA-PATRIOT Act—including the authority to run checks on an individual's library use. Civil libertarians expressed alarm that the act, which had been passed to protect personal freedoms, was now being used to abuse those freedoms. Law enforcement officials complained that the standard of accountability demanded by the court was still too onerous and high. The nation's checks and balances were functioning as intended.

• • •

From the late 1940s onward, as the executive branch carried out its primary accountability responsibilities, Presidents issued classified and unclassified directives and executive orders making adjustments and interpretations to the 1947 National Security Act. In 1956, the Eisenhower administration created the President's Board of Consultants on Foreign Intelligence Activities, which became the President's Foreign Intelligence Advisory Board, a board of citizens from outside the government charged with providing the President with advice on the performance of the intelligence community and recommendations for improving that performance.[15]

These executive branch changes came into sharper, more prominent focus in the mid-1970s coincident with the congressional hearings and establishment of the House and Senate Committees. Executive Order 11905 on U.S. Foreign Intelligence Activities, signed by President Ford on February 18, 1976, and Executive Order 12036 signed by President Jimmy Carter on January 24, 1978, not only codified the authorities and responsibilities of the DCI and the institutional members of the intelligence community but also included a major section titled "Restrictions on Intelligence Activities." Both orders carried explicit language prohibiting assassination.

Executive Order 11905 established a new Intelligence Oversight Board charged specifically with examining and reporting to the President on an intelligence action or actions that might be either unlawful or contrary to executive branch directives.[16] The Carter executive order retained this new board while eliminating the President's Foreign Intelligence Advisory Board. On December 4, 1981, President Ronald Reagan in signing intelligence Executive Order 12333 stated: "Let us never forget that good intelligence saves American lives and protects our freedom." With the new order, the pendulum of accountability swung from restrictions on intelligence to the importance of the full and effective functioning of intelligence. Section 2.1 of the order stated:

> Accurate and timely information about the capabilities, intentions and activities of foreign powers, organizations or persons and their agents is essential to informed decisionmaking in the areas of national defense and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.[17]

The Reagan administration reestablished the President's Foreign Intelligence Oversight Board, which continues today. Executive Order 12333 remained in effect up to the government's intelligence reform actions in the post-9/11 era.

POLITICIZING AND IRRELEVANCE

The American intelligence professional operating within the framework established by the three separate branches is expected to be a figure of absolute integrity. It was with this in mind that the National Security Act of 1947 made the Director of Central Intelligence, or DCI, an advisor rather than a full member on the National Security Council. The intelligence officer is looked to for both strategic and tactical warning of events that may occur, to offer the best data and best judgments on an intelligence target's capabilities and intentions. The intelligence officer is expected to state what is known, what is not known, and what in his or her judgment is the best estimate of the situation. In this vital role, he or she can expect to be the occasional skunk at the garden party offering advice contrary to that which the policy maker or operational commander would prefer to hear.

Under the U.S. scheme of intelligence accountability, the intelligence professional must not slant or bend data and estimates to suit the preference of the consumer. This is true, as well, during the collection and analysis stages of the work inside the intelligence community. The intelligence cannot be slanted to curry favor or keep the peace with someone more senior in the intelligence chain. To do so is to politicize the intelligence, and this is unacceptable.

During his 1991 Senate confirmation hearings for the post of DCI, Robert M. Gates was met with allegations that as a CIA professional he had politicized intelligence analyses on the Soviet Union. In preparing for his testimony to the Committee, Gates reviewed the scores of intelligence assessments relevant to the charges raised. He wrote:

> After I had dealt with the specific allegations, I told the committee: "... A careful review of the actual record of what was published and sent to policymakers demonstrates that the integrity of the process was preserved. We were wrong at times, but our judgments were honest and unaffected by a desire to please or slant. ... I had and have strong views. But ... I'm open to argumentation and there was a lot of that. And I never distorted intelligence to support policy or to please a policymaker."[18]

Gates was confirmed and delivered an address to the CIA's analysts on the importance of guarding against politicizing intelligence early in his tenure as DCI.

Following the 2003 invasion of Iraq, charges and countercharges flew over whether the U.S. intelligence community had distorted intelligence pointing to weapons of mass destruction in Iraq. President Bush established the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass

Destruction to investigate. In its covering letter to the President forwarding their findings, the commissioners wrote, in part: "We conclude that the Intelligence Community was dead wrong in almost all of its pre-war judgments about Iraq's weapons of mass destruction. . . . After a thorough review, the Commission found no indication that the Intelligence Community distorted the evidence regarding Iraq's weapons of mass destruction. What the intelligence professionals told you about Saddam Hussein's programs was what they believed. They were simply wrong."[19]

• • •

Although intelligence must not be slanted or distorted to suit the preferences of the consumer, it must have relevance to the needs of the consumer. From 1952 to 1967, Sherman Kent chaired the CIA's Board of National Intelligence Estimates. Kent believed deeply in the integrity of the intelligence estimates process. The work had to be of the best possible quality.

When the estimate was published, the burden, in Kent's view, shifted to the policy maker. "Let things be such that if our policy-making master is to disregard our knowledge and wisdom," Kent said, "he will never do so because our work was inaccurate, incomplete, or patently biased. Let him disregard us only when he must pay greater heed to someone else. And let him be uncomfortable—thoroughly uncomfortable—about his decision to heed the other."[20] In editing Kent's essays on intelligence, Donald Steury examined the decline and eventual demise of the Board of National Intelligence Estimates and found that the board had difficulty focusing on policy makers' priority interests. "The reverse of Sherman Kent's coin of detached objectivity was irrelevance."[21]

If Kent and his board slowly slipped into irrelevance from the 1950s to the 1960s, bear in mind that their decline was set in the printed, hard-copy, pre–information age, when the intelligence community often was the only reliable source on foreign target information. The sources of information available to today's policy-level consumer of intelligence—whether dealing with the Russian Federation rather than the Soviet Union or with any of the current era's closed societies—are far, far greater than forty years ago.

It is almost a given that today's policy-level consumer is quite well informed in his or her area of interest and not dependent on an analyst for a continuing stream of routine, updating information. The analyst no longer sets the pace of the information flow. The web, the media—electronic and hard copy, U.S. and foreign—the telephone, the fax, the interaction with U.S. and foreign colleagues in the professional field, and intelligence reporting available at the consumer's personal, classified, computer keyboard—all play a part.

Today's analyst must not only have a sense of his or her consumer's level of continuing information and knowledge. To provide value-added analysis, today's analyst must focus more sharply on the specific needs and timing of meeting those needs for the policy-level consumer, seek specific tasking, analyze feedback from analysis already provided, and invite and tackle the consumer's hard questions demanding answers.[22]

Today's combatant commanders place a far higher priority on intelligence and demand far more from intelligence than was the case in the Cold War era. The formerly dominant challenges of understanding force-on-force foreign military capabilities and intentions have been subsumed in a far broader spectrum of intelligence challenges and requirements. In a cyber- and information-era world marked by failed and failing nation-states, religious and cultural conflicts, the proliferation of weapons of mass destruction, and virulent international terrorism, defense intelligence must have an appreciation of regional cultures, religions, and politics, as well as the smoldering tinder of intentions and the sparks of conflict.

In a strategic environment where U.S. forces with their allied and coalition partners are called on to provide forward deterrence, produce forward stability, and ward off threats to the U.S. homeland, there is virtually no geography, no political, cultural, ideological, or religious presence anywhere that is not of relevance. Today's commander holds defense intelligence accountable for the development of increasingly agile, flexible, fused collection and analysis capabilities that allow swift transformation of data into knowledge, for working in partnership with operations, with swift delivery of that knowledge.

UNSAVORY CHARACTERS

The moral dimensions of the work of U.S. intelligence have brought into the focus the question of what types of foreigners Americans should deal with in carrying out the intelligence mission. In espionage, the handling of spies, the turning of agents, and the infiltration and exfiltration of agents are at the heart of intelligence collection and intelligence operations. The challenges such operations pose, the skills they require, the stresses they place on those responsible for their conduct are uniquely challenging. People—however varied, laudable, or sordid their motives and their backgrounds—inform, betray, and ferret out information critical to intelligence successes. Identifying, cultivating, and running such people take time, money, and professional management of the first order. It can be a rough, risky business.

The chair of the House Permanent Select Committee on Intelligence, Representative Porter Goss (R-FL), observed in 2002 that in the mid-1990s,

> The world's remaining superpower—the USA—was losing sight of the contributions made by the Intelligence Community, our first line of defense, our eyes, and ears, and brain. . . . For example, human intelligence capabilities were hampered by policy guidance that place a higher priority on ensuring that assets weren't tainted with human rights abuses rather than on what information they may have had or may have been able to get.[23]

Goss was referring to a pronouncement by the new DCI John M. Deutch in 1995 that he would be establishing fresh guidelines for CIA dealings

with alleged killers, torturers, human rights violators, and other unsavory characters.

Deutch was responding to allegations that CIA agents had been too closely involved with such types and that this contact was not consistent with American interests and values. His critics charged he was producing a risk-adverse atmosphere at the very time when information on terrorist intentions from whatever source was vital to the nation's defenses. Two days after the terrorist attacks of 9/11, Congress directed the DCI to rescind the guidelines. In October 2001, the USA-PATRIOT Act "expressed the sense of the Congress that intelligence officials 'should be encouraged, and should make every effort to establish and maintain intelligence relationships with any person, entity, or group to acquire information on terrorist groups.' "[24]

Here the voice of the late Rebecca West, as expressed in her book *The Meaning of Treason,* provides sage advice for those grappling with accountability. "Not until the Earthly Paradise is established and man regains his innocence, can a power which has ever been at war be blamed if it accepts information regarding the military strength of another power, however this may be obtained; and of course it can be blamed least of all if the information comes to it from traitors, for then it is likely to touch on the truly secret."[25]

DEMOCRATIC PRINCIPLES

The truly secret comes not only from traitors but also from code breakers. The truly secret involves deception on the grand scale. The issues of stealing the communications of and deceiving others find their accountability places in the U.S. intelligence morality play.

In World War I, Herbert O. Yardley, a State Department code clerk, moved to the Army to establish the MI-8 Branch of the Military Intelligence Division, a branch dedicated to collecting and decrypting foreign communications. At the end of the war, Yardley arranged for Army and State jointly to fund a continuation of the code-breaking operations. He and his staff had considerable success, including breaking the Japanese code at the time of the 1921 Washington Naval Conference.

Yardley's success was measured against a fresh standard of accountability in 1929 when a new Secretary of State, Henry L. Stimson, took office. When he became aware of the decryption operations, Stimson was deeply disturbed. "The chief lesson I have learned in a long life is that the only way you can make a man trustworthy is to trust him; and the surest way to make him untrustworthy is to distrust him and show him your distrust. We can do better by being an honest simpleton in the world of nations than a designing Sherlock Holmes. . . . Gentlemen do not read each other's mail." He ordered the State Department's funds for the code breaking stopped immediately. When the *Philadelphia Public*

Ledger learned of Yardley's work, it denounced the decryption of diplomatic messages as discreditable.[26]

Fortunately for the nation, this puritanism stopped short of the separate work under way in the Army and the Navy against Japanese codes that continued throughout the 1930s. Code breaking was extraordinarily difficult, time-consuming work. The Army cracked the Japanese diplomatic code in 1940. The Navy was working hard on the Japanese Fleet General Purpose code. In March 1942 there was a breakthrough allowing current decryption of operational orders to the Japanese fleet.[27] The U.S. Pacific Fleet was still reeling from the December 7, 1941, surprise attack on Pearl Harbor. The Navy needed to know where the Japanese were planning to strike next in the Pacific—possibly New Guinea–Solomons, Australia, Midway Island, or the U.S. mainland.

Cmdr. Joseph Rochefort was the Navy code breaker in charge of a unit serving under Adm. Chester W. Nimitz at Pearl Harbor. In May, a partial decrypt translating as "invasion force" was followed by the geographic designator AF. Rochefort and his team deduced that AF stood for Midway Island. Were the Japanese planning to strike and capture Midway? If the aircraft carriers of the U.S. Pacific Fleet were to be positioned correctly, the Navy needed confirmation.

With Nimitz's approval, Rochefort had a message sent via secure undersea cable from Hawaii to the U.S. forces on Midway instructing them to send a clear, uncoded flash message advising that Midway's water distillation plant had broken. Two days later, the U.S. Navy code breakers decrypted a Japanese fleet message advising that AF had only a two-weeks supply of fresh water. Subsequent Japanese messages indicated the likely date and direction of the attack.[28] This signals intelligence coup allowed Nimitz to surprise the Japanese force under Adm. Chuichi Nagumo. The Battle of Midway was joined on June 4, 1942. By the morning of June 5, all four of the Japanese carriers had been sunk, with the United States losing a single carrier. Signals intelligence (SIGINT) had played a vital role in swinging the tide of battle in the Pacific.[29]

Intelligence had played a crucial role at an extremely fragile point in the nation's history. SIGINT grew into an enormous intelligence discipline in the post–World War II, Cold War era. The Soviet Union was the primary target. The Army and Navy SIGINT services merged into the new National Security Agency (NSA) in 1952. More than fifty years later, NSA's role in the post-9/11 era is crucial, evolving dramatically as the nation blends foreign and domestic intelligence into national intelligence.

In his April 2005 confirmation hearings to become the first principal Deputy Director of National Intelligence, Gen. Michael V. Hayden, who was finishing his sixth year as NSA Director, told the Senate Committee, "American intelligence agencies needed to push 'right up that line,' established under privacy laws in using eavesdropping, surveillance, and other tools to gather information." He told the Committee that it would be vital to ensure "that we are not pulling punches, that we are using all the abilities that Congress has given us under the

law. We all know that the enemy may be inside the gates and Job One is to defend the homeland."[30]

• • •

Taking measures to block, prevent, or impair collection of information—*denial* and deliberately manipulating information to mislead, *deception*—have been part of statecraft and warfare from the beginning of states and battles.

Early in World War II, as part of the great game of intelligence, the British exercised tactical deception to considerable advantage. The goal in deception is to influence not only what your opponent thinks but, more important, what your opponent *does*. In the North African campaign and the Battle of Alam Halfa, British intelligence from several sources indicated that the German forces had poor knowledge of the battlefield terrain. "The allies knew that the sands in and around the Ragil depression would not support armored vehicles. . . . Eighth Army cartographers made a 'false-going' map that showed good hard ground in the Ragil area. The deception was implemented by putting the map in a vehicle deliberately disabled in a minefield. German scouts retrieved the map and delivered it up the chain of command."[31]

When Roosevelt, Churchill, and Stalin met in Tehran, preparations for the 1944 Allied landings in France (Operation OVERLORD), were on the agenda. Churchill asked about the deception and propaganda cover plan, observing that truth deserves a bodyguard of lies.[32] BODYGUARD became the title of the OVERLORD deception plan. When the plan had been drafted, U.S. and British officers flew to Moscow in early 1944 to brief it to the Soviets and obtain their agreement and their plans for cooperation. The Soviet Lt. Gen. Fedor F. Kuznetsov was their principal interlocutor. After weeks of delay, he advised that BODYGUARD was accepted completely. It was when discussion turned to implementation of the deception that the issue of what was acceptable and not acceptable surfaced. The American and British officers "chatted with Kuznetsov about using the press for deception, making it clear that the Western Allies did not do so . . . when we said that in a democracy you couldn't use the press to fool your own people, the Soviets said 'Oh, well, we do it all the time.' "[33]

Sixty-one years later, in December 2005, when news stories surfaced that the U.S. command in Baghdad was paying Iraqi newspapers to run positive stories about the state of play in Iraq, feathers immediately flew in Washington. The chair of the Senate Armed Services Committee expressed grave concern and advised that the Department of Defense was looking into the situation. Few disagreed that it would be unethical to run such stories in the U.S. media, but debate was joined on question of "mitigating circumstances justifying such tactics in Iraq."[34] After several weeks of review, an inquiry found in early 2006 that no policy had been violated or laws broken by the news story actions. This said, the Department of Defense announced that it would review whether updated policy guidance was needed.[35]

THE TWO-SIDED COIN

In these early years of the twenty-first century, intelligence is held accountable on the one hand for errors, failures, and wrongdoings and on the other hand for the demonstrated increases in its capabilities and the growing excellence of its performance. During the Balkans conflict, a year after the mistaken 1999 bombing of the Chinese embassy in Belgrade in the belief that it was the headquarters of Yugoslav Army Procurement, the CIA officer responsible for error was dismissed by the DCI, and six other employees were disciplined.[36]

On a grander scale, the House-Senate committee investigating the 9/11 terrorist attacks called on the CIA inspector general "to determine whether and to what extent personnel at all levels should be held accountable for any omission, commission, or failure to meet professional standards." Following his investigation, the inspector general recommended that the CIA Director convene an accountability board. After a lengthy review, Director Porter Goss determined in October 2005 that he would not seek to hold current or former officials responsible for failures leading up to the attacks.[37] In a formal statement, the Director of National Intelligence concurred with this decision, saying he would work with Goss and the CIA to continue to address the systemic issues involved.[38]

The war on terrorism has brought fresh expectations of intelligence—expectations of enormous dimensions. At the same time, the war, which pits nation-states against individuals, cells, and nonstate actors bent on the most murderous of designs, has brought changes to the ground rules for intelligence. New questions, along with differing interpretations of the acceptability (or lack thereof) of intelligence's role in capturing, interrogating, imprisoning, and condoning torture by other nation-states of terrorists, have brought vivid new strokes to the accountability canvas.

In December 2005, Congress entered into a heated debate on renewal of the USA-PATRIOT Act with proponents arguing that the war on terrorism requires continued approval of expanded surveillance authorities and with opponents firm in their belief that such authorities violate basic civil liberties. In the middle of this debate, the *New York Times* reported, in a story it had been holding unpublished for a year, that in 2002 the President had signed an order authorizing—without the requirement for a warrant from the FISA Court—the monitoring of international telephone calls and e-mails of people inside the United States to track suspected terrorist agents and "dirty numbers" linked to Al Qaeda.[39]

The President was firm in underscoring the correctness of his surveillance order, stating that as President and Commander-in-Chief he had the constitutional responsibility and authority to protect the country, that his authorization of the intercept of international communications was consistent with U.S. law and the Constitution, and that "to save American lives, we must be able to act fast and to detect these conversations so we can prevent new attacks."[40] In parallel, the Director of National Intelligence, in a message to intelligence community colleagues, stated, "Last week we witnessed an egregious disclosure of classified

information regarding one of our country's major tools in the War on Terror—the interception of al-Qa'ida-related communications. . . . Despite this setback, given the program's continuing utility to the War on Terror and its proven effectiveness in disrupting terrorist threats to the homeland, we will continue to pursue this and other critical efforts."[41] Certain members of Congress challenged the legality of the order; others said that hearings would be held. The nation's checks and balances clearly were in action.

After vigorous debate early in 2006, the Senate and the House voted favorably on renewal of the USA-PATRIOT Act will its provisions largely intact, and on March 9, 2006, the President signed the renewed act into law. In parallel on the issue of wiretap surveillance, by late March 2006, separate pieces of draft legislation had been introduced in the Senate that variously would give the President a set period of time to conduct wiretaps before seeking authorization from other branches of the government or would ease FISA Court restrictions for such wiretapping.[42]

Within the intelligence community, under the leadership of the Director of National Intelligence, the accountability focus is on increased capability and excellence of performance. Top priority is given to bringing foreign and domestic intelligence cultures together to provide the delivery of effective national intelligence. The mindset is on taking risks, not risk avoidance. The strategic mission objectives focus on defeating terrorists at home and abroad, preventing and countering the spread of weapons of mass destruction, bolstering the growth of democracy and democratic states, developing innovative ways to penetrate and analyze the most difficult targets, and providing intelligence that anticipates issues of concern and opportunities for decision makers.[43]

Across the nation, if intelligence was first formally declared an instrument of U.S. national security in the National Security Act of 1947, it did not enter the mainstream of American thinking and discourse until the terrorist attacks of 2001 and their aftermath. With the shock and continuing fear engendered by the attacks, and with the extensive media coverage and debate relating to the post-9/11 commission studies and the passage of the intelligence reform legislation, millions of Americans have come to understand that timely, relevant intelligence is "the air the nation breathes," information essential to our survival and well-being.

In a steadily growing number of colleges and universities across the nation, the history, role, and contributions of intelligence are recognized as an important academic field of study and research. The burning of effigies of intelligence leaders on campus is history. It is no longer adequate to relegate the study of intelligence to an examination solely of the negative "rogue elephant" chapters in intelligence history. Intelligence departments are being formed. Intelligence degrees are being offered. The interests of college students extend beyond the classroom to the prospect of intelligence as a career.[44] We are arriving at point in the nation's history where more citizens are coming to the realization that intelligence is too important to be left solely to the government's checks

and balances. If Americans are to have the essential contributions that intelligence brings to their safety and security, citizens across the land are accountable for ensuring that the government is providing for that intelligence in full measure.

NOTES

The views expressed are those of the author and do not represent the official views of either the Department of Defense or the U.S. Government.

1. Letter from General George Washington to Col. Elias Dayton, July 26, 1777, original letter in Pforzheimer Collection, as quoted in address by Walter L. Pforzheimer to the Grolier Club of New York, published in Hayden B. Peake and Samuel Halpern, eds., *In the Name of Intelligence, Essays in Honor of Walter Pforzheimer* (Washington, DC: NIBC Press, 1994), p. 73.

2. Dwight D. Eisenhower, *Crusade in Europe* (New York: Doubleday, 1948), p. 32.

3. Omar Bradley, *A Soldier's Story* (New York: Modern Library, 1999), p 33.

4. Robert Hayden Alcorn, *No Bugles for Spies* (New York: David McKay, 1962), p. 195.

5. See A. Denis Clift, *Clift Notes,* 2nd ed. (Washington, DC: Joint Military Intelligence College Press, 2002), pp. 109–11.

6. Boren Hearings for Webster's confirmation as DCI, Senate Select Committee on Intelligence, Washington, DC, April 8. 1987.

7. John Ranelagh, "Through the Looking Glass: A Comparison of United States and United Kingdom Intelligence Cultures," quoted in Peake and Halpern, eds., *In the Name of Intelligence* p. 425.

8. President George W. Bush, Address to a Joint Session of the Congress, Washington, DC, September 20, 2005.

9. Intelligence Reform and Terrorism Prevention Act of 2004, 108th Congress, 2nd sess. (January 20, 2004), Washington, DC.

10. John D. Negroponte, *The National Intelligence Strategy of the United States of America* (Washington, DC, October 2005).

11. James Van Wagenen, "Congressional Oversight: A Look Back," *Studies in Intelligence* 1, no. 1 (1997), quoted in paragraph from Clift, *Clift Notes*, p. 108.

12. Ibid.

13. Ibid.

14. Loch K. Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (Lexington: University Press of Kentucky, 1985), preface.

15. See http://www.cia.gov/publications/facttell/exectuve_oversight.html 12/8/05.

16. Ibid.

17. See http://www.cia.gov/cia/information/eo12333.html 12/08/05.

18. Robert M. Gates, *From the Shadows* (New York: Simon & Schuster, 1996), pp. 547–50.

19. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005, Forwarding Letter (Washington, DC: Government Printing Office, 2005).

20. *Sherman Kent and the Board of National Estimates, Collected Essays*, edited by Donald P. Steury (Washington, DC: Center for the Study of Intelligence, 1994), p. 34.

21. Ibid., p. xx.

22. See Carmen A. Medina, "What to Do When Traditional Models Fail," *Studies in Intelligence* 45, no. 4 (2001), pp. 35–40, cited in Clift, *Clift Notes*, pp. 203–4.

23. Porter J. Goss, "Commencement Address," Joint Military Intelligence College, Washington, DC, August 9, 2002.

24. Richard A. Best, CRS Issue Brief for Congress, "Intelligence Issues for Congress," Library of Congress (November 9, 2001).

25. Rebecca West, *The Meaning of Treason* (London: Phoenix Press, 2000), p. 192, as cited in A. Denis Clift, "Keynote Address," Swedish National Defense College, Stockholm, Sweden, August 27, 2003.

26. David Kahn, *The Reader of Gentlemen's Mail* (New Haven, CT: Yale University Press, 2004), pp. 98 and 102.

27. Stephen Budiansky, *Battle of Wits* (New York: Free Press, 2000), p. 12.

28. Ibid., pp. 14–16.

29. E. B. Potter, *Nimitz* (Annapolis, MD: Naval Institute Press, 1976), p. 107.

30. Douglas Jehl, "No. 2 Intelligence Nominee Testifies on Privacy Rules," *New York Times* (April 15, 2005), as cited in A. Denis Clift, "Doing Our Work Differently, Doing It Better" Rand Symposium, Washington, DC, June 15, 2005.

31. Neal D. Norman, "British Intelligence and Information Superiority at the Battle of Alam Halfa: Turing the Tide in North Africa," master's thesis, Joint Military Intelligence College, Washington, DC (1997), pp. 78–80, as cited in Clift, *Clift Notes*, pp. 56–57.

32. Keith Eubank, *Summit at Teheran* (New York: William Morrow, 1985), p. 338.

33. Thaddeus Holt, *The Deceivers* (New York: Scribner, 2004), pp. 517–18.

34. Josh White and Bradley Graham, "Military Says It Paid Iraq Papers for News," *Washington Post*, December 3, 2005, p. A1.

35. Thom Shanker, "No Breach Seen in Work in Iraq On Propaganda," *New York Times*, March 22, 2006.

36. Steven Lee Myers, "Chinese Embassy Bombing: A Wide Net of Blame," *New York Times*, April 17, 2000. p. A1.

37. Dafna Linzer and Walter Pincus, "CIA Rejects Discipline for 9/11 Failures," *Washington Post*, October 6, 2005, p. A1.

38. Statement by Ambassador John D. Negroponte, Director of National Intelligence, ODNI News Release No. 1-05, October 5, 2005.

39. James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times* (December 16, 2005), p. A1.

40. Press Conference of the President, December 19, 2005, available at http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html.

41. Director of National Intelligence, Letter to Intelligence Community, Washington, DC (December 19, 2005).

42. Eric Lichtblau, "Judges on Secretive Panel Speak Out on Spy Program," *New York Times* (March 29, 2006), p. A19.

43. Negroponte, *The National Intelligence Strategy*, pp. 1–4.

44. See A. Denis Clift, *Learning with Professionals, Selected Works from the Joint Military Intelligence College* (Washington, DC: Joint Military Intelligence College Press, 2005), p. v.

9

A HALF CENTURY OF SPY WATCHING

HARRY HOWE RANSOM

SINCE SEPTEMBER 11, 2001, A PUBLIC PREOCCUPATION and controversy was rekindled about the function, performance, and controls of America's secret intelligence system. Since its creation in 1947, the Central Intelligence Agency (CIA) has periodically been the subject of intense public debate about its proper role and control in American government. Its special status has required it to struggle for legitimacy.

This has prompted me to reflect on my long academic journey as a student of America's intelligence establishment. This chapter will briefly survey my experience of the past half century in attempts to understand this secret side of government and how the CIA has interacted with the American political system and democratic values.

In the face of an accelerating technology and a rapidly changing world, intelligence information has never been more important to national security. And it is to the intelligence establishment we depend on to define and warn of threats to the nation's security. This gives the intelligence system enormous potential power to determine policy and action in foreign affairs. And the unavoidable secrecy protecting the system poses obstacles to the accountability that American democracy demands. The nation's founders created a system of checks and balances—the separation of executive, legislative, and judicial authority—to promote accountability to the people. The dynamic interplay of secrecy and accountability became the focus of my studies.

Many wonder: What do political scientists *do*? The best answer, albeit simplistic, is that we study power in a governmental context. As a sophomore at Vanderbilt University thinking about majoring in political science, I recall choosing as a topic in a public speaking course, Military Intelligence. I must have

been intrigued, back in 1941, by the idea of applying information to government security policy and action. I suspected that knowledge—intelligence—is a crucial element in the governmental policy process.

My World War II Army assignments involved no experience with military intelligence. After the war for a few years I was a first lieutenant in Army Intelligence Reserve. But the Army never exposed me to any secrets. I have had no hands-on government experience or access to classified data in intelligence. In my graduate study at Princeton University, I ultimately focused on the broad topic of civil-military relations. My doctoral dissertation was an analysis of the role of Congress in determining military aviation policy after World War I. I was interested in the interplay of congressional politics and armed services politics. The impetus for this choice of topics was a concern with civil-military relations, or as it was sometimes put in the context of American constitutional democracy, "civilian control of the military."

Although this issue was not directly related to intelligence questions, my interest was prompted in 1955, when I was invited to Harvard University to help create a Defense Studies Program supported by a Ford Foundation grant. At Harvard, I began seriously to study the government's foreign intelligence system. It seemed critically important to be informed about how the government was organized for gathering information for Cold War national security policy making. Part of my assignment was to develop reading materials for Harvard graduate students enrolled in a large academic year-long Defense Policy Seminar. Very little literature was available about the CIA, which by the mid-1950s had become a large government organization.

Several dozen students were enrolled from the Harvard graduate schools of Public Administration, Law, and Business. Our charge was not only to operate a year-long seminar in defense policy but also to create and assemble teaching materials on the various segments of the national security establishment. The literature was thin and scattered, especially about strategic intelligence. At this point I undertook the assignment to cover the CIA and other parts of what was called the intelligence community. I soon learned that such a label as "community" was more aspiration than reality. I also learned that very little scholarly information was available on the subject.

As a political scientist studying power, I soon learned that this massive secret intelligence apparatus engaged not only in spying but also in a variety of covert actions, including psychological warfare and political intervention overseas. These activities presented special problems for American constitutional government. Obviously, problems existed of accountability, congressional knowledge and control, and balance between the legislature and executive. Other problems included ethics, morality, civil liberties, and respect for domestic and international law. I shared Lord Acton's concern in his often quoted phrase: "Power corrupts; secret power [Acton said absolute power] corrupts absolutely."

In simplest terms, on the one hand, government espionage and other covert operations require secrecy. Democratic government, on the other hand, requires

public accountability. Can these conflicting requirement be accommodated? I wondered. And I still wonder. With this question in mind, I set about to collect information about the CIA for students in the Defense Policy Seminar. I was advised at every turn that this subject could not be studied in a systematic scholarly way because the relevant information is secret. Although secrecy was a major problem, one encounters many other issues inhibiting study of this subject. Let me mention two more complications that obscure a realistic assessment of secret intelligence.

First, there is the semantic entanglement of intelligence terminology. Put simply, we encounter a very ambiguous vocabulary. The principal terms are often used interchangeably and incorrectly. What are these terms? Essentially, *intelligence* means information. Espionage, or spying, is a way of stealing information. Like stealing, espionage is illegal and must be pursued deceptively in secret. Counterintelligence is a police and security activity, aiming to protect the secrets of one's own nation from spies. Covert action, sometimes called covert operations or special activities, means secretly intervening by various means in the political affairs of other nations to produce a desired outcome. Although covert action is not strictly speaking an intelligence function, it is generally performed within an organization called an intelligence agency. Most often misused are the words *agent* and *spy* when referring to a case officer or analyst. But all of these terms often are used interchangeably and imprecisely. Newspaper headlines are particularly prone to confusion of the terms.

A second impediment to public understanding of this subject is the romanticized image of intelligence professionals presented in popular works of fiction. Ian Fleming's novels and movies about James Bond translate secret agentry into heroic deeds. To a reader Bond is a spy. In fact, he rarely engages in espionage. Rather, Bond's adventures resemble counterintelligence or covert action. I argue that covert operations are separate and distinct from the intelligence function. Yet one historian has invented a term, *jamesbonderie*, for a perception that has come to dominate and confuse public understanding of intelligence.[1]

Tom Clancy's fictional protagonist Jack Ryan is another example of a popular hero whose activities further confuse the semantics. The fictional Ryan has a doctorate in history and serves in and out of the CIA in important positions. His exploits as a CIA "superman" bear no more resemblance to reality than the deeds of Clark Kent. Closer to reality, perhaps, are the more subtle novels of British author David Cornwell (who writes under the pen name of John Le Carré). His novels portray intelligence work and espionage as a dull, sordid, immoral, and ultimately pointless game. Although Le Carré's novels may be somewhat more realistic than those of Clancy or Fleming, they are harshly cynical. My point is that government secrecy and disinformation, media sensationalism, imprecise vocabulary, and fictional romanticism combine to obscure comprehension of intelligence, both for the public and even for a scholar who seeks to clarify the subject.

Official secrecy was a major obstacle to my research from the start. Nevertheless, I set about to apply the principles of intelligence analysis—fitting together bits of information—from library resources, newspapers, congressional documents, and from those few leaders within the intelligence system willing to talk with me. My task was to connect the dots. Among the most helpful personal guides to accurate information in the late 1950s were two high CIA officials: William Bundy and Robert Amory. But my primary viewing point of the system was from the ivory tower. I was able to produce publishable manuscripts that passed the test of prior scholarly review. My first book, published by Harvard University Press in 1958, evoked a surprising amount of public attention,[2] which was due less to the book's merit than to the fact that no other serious scholar had attempted to describe in such detail the large intelligence bureaucracy that had grown in the first decade of the Cold War. When my book because a best-seller in the Washington, DC, area during 1958–59, I wondered whether the CIA was buying up copies and burning them. Thirty-five years later, I learned (to my surprise) that my book had received a favorable review in CIA's secret in-house journal. Allen W. Dulles, one of the CIA's founding fathers, once told me that my book had been "useful."

Viewing the CIA and the intelligence system half a century later, the change is dramatic. In 1956, little public knowledge existed about the system. Rarely did the CIA appear in news headlines. Few persons could name the CIA's director or be able to distinguish the agency's function from that of the Federal Bureau of Investigation (FBI). Occasional derring-do articles appeared in the press by investigative journalists under headlines such as "Fighting the Cold War Under Cover." University courses on strategic intelligence were nonexistent. Any attempt to assemble a bibliography of authoritative contemporary publications was virtually impossible.

More than half a century after its creation, the CIA became an almost daily topic in press headlines. This has been especially so since the surprise terrorist attacks on September 11, 2001. Now library shelves bulge with current books on intelligence and various aspects of the "CIA problem." Scores of memoirs and biographies of intelligence officials, including most former Directors of Central Intelligence, are available today.

Today the study of intelligence has become an academic speciality and an extensive, ever-expanding bibliography is available. Early on, the CIA created its own Center for the Study of Intelligence. It publishes informative articles in both classified and nonsecret versions and maintains a website with detailed information about its organization and functions. Also provided is an extensive bibliography of nonsecret publications on intelligence. More recently, a CIA University has been established, as well as the Sherman Kent School of Intelligence Analysis. In Washington, DC, a popular tourist site is the nongovernmental International Spy Museum. Its stated purpose is "to educate the public about espionage in an engaging manner and to provide the dynamic context that offers an understanding of its important role and impact on current and historical

events." A CIA program sends selected intelligence officials to serve as visiting faculty at selected universities. The Agency has conducted several conferences at its Langley headquarters to which civilian academic specialists were invited. The CIA maintains a website with detailed information about the agency's organization and functions as well as a CIA's Home Page for Kids. These developments have increased the opportunities for effective oversight, but the record has remained uneven.

Today library shelves are crowded with an almost overwhelming number of studies by presidential, congressional, and private research groups on problems of intelligence policy, organization, and performance. These constitute one of the principal forms of information about the government's secret intelligence apparatus. Few agencies of the federal government have been as perpetually controversial as the CIA. Yet the question persists: How adequate have been efforts at oversight? How truly accountable has the secret intelligence system been to those responsible to the public within the nation's democratic framework?

In spite of the large volume of hearings, studies, and reports, layers of secrecy remain on some of the most critical issues of oversight and accountability. We remain essentially in the dark about some questions of use and abuse of intelligence prior to 9/11. Many of the studies focus on the performance of the intelligence system and how well it served decision makers in an objective fashion. My own interest in this subject evolved from my initial concern about the conflict between our government's desire to gain legitimate information affecting national security and democratic principles of accountability. In spite of the changes in availability of information about the CIA that I have described, this conflict persists.[3]

The American democratic ideal rests on the assumption that the people are the ultimate source of authority and are to be governed with their informed consent. Applying this ideal requires openness and disclosure. But many aspects of national security—military, diplomatic, and intelligence—sometimes require a high degree of secrecy. How can some governmental systems be popularly controlled by those who cannot see? The story of secret intelligence in a democracy has been the story of efforts to reconcile these competing requirements. At this writing, intense controversies exist about various aspects of intelligence programs. Important among these are the prewar information about Iraq, use of torture to obtain information, detention of suspected terrorists, intrusive methods that include spying on Americans, and the persistent issue of politicization of intelligence.

Now I turn to some of my major specific concerns about the CIA as they have changed over the years. I illustrate five major concerns with specific examples from past observation and experience.

The first concern was the absence of effective legislative knowledge and control of the intelligence system. When the CIA was established in 1947, little thought was given to the role of Congress in overseeing intelligence activities. Through the power of the purse, the Constitution gives Congress complete control

over all government-funded activities. This is one way democratic accountability is supposed to work. But for two decades Congress was a sleeping, toothless watchdog. A handful of congressional leaders was assigned to monitor the CIA. But there was little payoff in their home districts or party positions for aggressive oversight of a secret entity within the executive branch. They could not publicly discuss their work. They saw their job as primarily to protect the agency. In my earliest writing I had proposed a Joint Congressional Committee on Intelligence with strong monitoring authority over all aspects of intelligence operations. Efforts were made in Congress toward this end. All failed. Similar proposals resurfaced over the years but all have run counter to the culture of Congress. The separation of appropriations and policy authority has been at the heart of the resistance to change, resulting in a system of oversight that is disbursed widely within the House and Senate.

In late December 1974, I was sitting in my office at Vanderbilt University. The telephone rang. On the line was Seymour Hersh, a *New York Times* investigative reporter with whom I was acquainted. "What would you say, Professor Ransom," Hersh queried, "if I told you that the CIA had been involved in a massive program of spying in the United States on Americans?" I expressed disbelief, noting that such activity is clearly prohibited in the CIA's legislative charter. In other words, such activity is illegal. On December 22, a few days after our telephone conversation, Hersh's front-page story detailing the CIA's domestic misdeeds appeared on page 1 of the *Times* and created a firestorm. Because Hersh quoted me in the article, I received many calls for comment from the national media. Surprisingly, few journalists seemed to understand that the CIA had no legitimate domestic security functions.

Within a few months the Senate and House began major investigations, by special committees, of the CIA's past covert activities, both foreign and domestic. The Church Committee in the Senate and the Pike Committee in the House undertook unprecedented hearings on intelligence operations. Additionally, a presidentially appointed commission, chaired by Vice President Nelson Rockefeller, undertook a parallel investigation of the CIA's misdeeds. Reports of these investigations spread details before the public about CIA-attempted assassinations of foreign leaders, opening of private citizens' mail, secret subsidies of foreign political parties, and hundreds of other formerly secret operations. The major consequence of these disclosures was the establishment of permanent committees in the Senate and House to oversee the intelligence establishment. For the first time, the CIA was circumscribed by a variety of controls and requirements that Congress be informed of intelligence and covert operations. Also prescribed was tightened presidential oversight. A clearly defined intelligence accountability to Congress was established. Even so, as later experience demonstrated, true accountability remained dependent on the willingness of Presidents and intelligence leaders to keep Congress properly informed. Secrecy gave special power to those who controlled secret information. So accountability continued to confront

secrecy. Over the years it has been aggressive journalists who have forced more accountability than Congress on the intelligence establishment.

My second concern is illustrated by what is known as the U-2 incident of May 1, 1960, when an American spy plane was shot down deep within the Soviet Union and its pilot, Francis Gary Powers, was captured. In a *New York Times Magazine* article published shortly after that event, I pointed out how the risks of such espionage missions and the costs to diplomatic aims might be greater than the benefits.[4] Speculatively, the United States might have achieved detente with the Soviet Union had President Eisenhower canceled U-2 flights prior to an upcoming peace conference in Paris among leaders of the United States, the Soviet Union, Great Britain, and France. Soviet leader Khrushchev canceled the conference because of the U-2 incident. Possibly he had other motives, including political pressures from home, but the spy plane provided an excuse. Biographers tell us that one of Eisenhower's greatest disappointments as President was the failure of the peace conference. Conceivably the Cold War might have ended thirty years earlier if not for this incident. At any rate, this example demonstrates that spying can sometimes conflict with diplomatic goals. The primacy of military espionage over diplomacy can produce unwanted results.

The third concern involves one type of politicization, illustrated by the example of the CIA-sponsored Cuban exiles' attempt to invade Cuba and overthrow the Fidel Castro regime in 1961. Prior to the headlines reporting the CIA's failed Cuban adventure, most Americans probably were only vaguely aware of the Agency's covert action capabilities. History books report this as the Bay of Pigs fiasco. President Kennedy immediately held himself accountable, which Presidents rarely do in such situations. This failed adventure prompted the *New York Times Magazine* editor to request that I write another essay.[5] My article suggested that the CIA failure at the Bay of Pigs was a consequence of housing intelligence analysis and covert action under the same CIA roof, but keeping them isolated from one another. I had long believed that an organizational mistake had been made back in 1947 by combining analysis and action. The Bay of Pigs project was a mistake and a failure because those favoring the invasion project insisted on information favoring its feasibility. In this case the information was cherry picked. And it was wrong. Castro was stronger than the project planners wanted to believe. Reportedly, the intelligence side of the agency was ignored by the covert operators.

Concern number four is closely related to the third: the tendency of intelligence agencies to supply information to please policy makers. I have called this problem politicization of intelligence. This is a somewhat complex matter. In simplest explanation, it involves making policy first and then demanding that the intelligence agency provide facts that support the policy. A long list of apparent intelligence failures have resulted from this tendency of intelligence professionals—particularly when facts are uncertain—to tell policy makers what they want to hear. Or alternatively, sometimes decision makers selectively hear only what they want.

Perhaps it is naive to believe that an agency charged with producing secret information can be insulated from partisan politics. After all, politics is about power, and information conveys potential power. Politicization is not usually a problem if there is broad consensus about foreign policy objectives. When consensus faded in the late 1960s over the Vietnam War, intelligence became a political football. Allen Dulles, one of the early influential intelligence leaders, liked to say, "We give information only, not advice." Perhaps that was once true. Indeed, information objectivity was one of the reasons for creating the CIA as an independent arm of presidency, detached from the military services or the State Department.

Politicization was brought home to me in the early 1980s in a brief conversation I had with then Director of Central Intelligence William J. Casey at CIA headquarters in Langley at an academic conference. I deliberately challenged him with this comment: "You have recently made a foreign policy speech at Westminister College in Missouri. I thought that CIA officials refrained from making foreign policy speeches." Taken aback, Casey hesitated for a moment and then told me, "Well, I have never agreed with that principle of detachment from policy." Then he added, "Besides, I am a member of the president's Cabinet." In my view, Casey and President Reagan had got it seriously wrong, as had some later Presidents. A CIA Director—or a Director of National Intelligence—should not be a member of the Cabinet and should be completely divorced from partisanship. Note that Casey had been Reagan's presidential campaign manager; his appointment as CIA Director was an inappropriate reward. Similarly, George H. W. Bush had been chairman of the Republican National Committee prior to becoming Director of Central Intelligence. Such appointments implied politicization. Casey's later efforts as CIA Director to operate outside of the nation's laws seriously affected the Agency's reputation as nonpartisan. A testimonial in this regard was the following statement by George Schultz, Reagan's Secretary of State: "I felt that the CIA's analysis was distorted by strong views about policy. . . . I had no confidence in the intelligence community."[6]

My fifth concern is about the future of the CIA. When the Soviet Union collapsed and a half century of Cold War ended, some raised the question, "Do we need the CIA?" In one sense the CIA was created in the mirror image of the Soviet security and intelligence: the KGB. Today there is no Soviet Union and a transformed KGB. One prominent senator, Patrick Moynihan, a former vice chairman of the Senate Select Committee on Intelligence, suggested that the CIA be abolished, proposing to turn over its intelligence functions to the Department of State. Op-ed pieces and newspaper editorials at one time called for the abolition of the CIA. Its reputation had been shattered by a series of scandals and apparent intelligence failures.

In 1994, Congress authorized yet another commission to study the organization, functions, and future of the intelligence system: the Aspin-Brown Commission. This action was precipitated in part by the end of the Cold War but primarily by the CIA's all-time worst internal scandals—the defection of one of

its officers, Aldrich Ames. Ames had struck a multimillion-dollar deal with the KGB to reveal bushels of secrets about CIA operations within the Soviet Union. Ames spent his ill-gotten rewards on an expensive home, luxury automobile, and high-end lifestyle. His undetected betrayal cost the lives of some dozen Soviet agents secretly working for the United States within the Soviet Union. CIA operations in Russia and Eastern Europe were virtually destroyed in the mid-1980s as a consequence of Ames's activities.

One is hard-put to explain how Ames's behavior could have been undetected for almost a decade. Perhaps a culture had developed within the Agency resembling a fraternity that assumed its members could do no wrong. Secrecy within the tightly compartmentalized CIA enabled Ames to betray his country undetected over a long period. Public revelation of his case caused a public relations disaster for the CIA. Editorial cartoons ridiculing the Agency numbered in the hundreds. The scandal came at the worst possible time for the CIA, when its competence was already being publicly debated and questions were being raised about its future.

Predictably, the CIA survived the Aspin-Brown Commission's study of its future, although major organizational reforms were proposed. The principle of a central agency independent of the various departments and federal agencies was seen as valid. Keep in mind that the CIA consumes only an estimated 15 percent of the intelligence system's estimated $44 million annual budget. Total budget figures remain secret in spite of widespread belief that budget totals should be made public. I have held the opinion over the years that half the annual budget is wasted. The trouble is, I do not know which half. Such is the price for inevitable secrecy. But certainly nothing is more rational and logical than that national security depends on the fullest degree of information available to decision makers. Yet much of this information inevitably is secret from the public. Intelligence misdeeds can now be reported without public disclosure. And inspectors general within the CIA and the National Security Agency now have authority to report misdeeds directly to Congress. In 1998 Congress passed the Intelligence Community Whistleblower Protection Act. Current or former intelligence employees can report misdeeds to Congress after raising concerns within their agency. Such reports remain secret. Since the Eisenhower administration, a President's Foreign Intelligence Advisory Board has existed. It operates secretly. Nonetheless, imperfections in methods for accountability over the years have left the CIA with a shaky legitimacy.

I have been impressed by an intelligence paradox. Recall that the United States entered World War II as a consequence of a spectacular intelligence failure at Pearl Harbor on December 7, 1941. This disaster was partly the result of various intelligence units failing to share crucial bits of information. There was no intelligence community. Yet World War II ultimately was won in large part because of the success of intelligence agencies in breaking enemy codes.

More recently I developed the controversial, speculative view that the Cold War arose out of a tragedy of faulty perception on both sides. On the one hand, perhaps there was a two-sided intelligence failure in which both the Soviet Union

and the United States misread the intentions of one another. On the other hand, accurate strategic intelligence may have prevented a global thermonuclear holocaust. This was the consequence of accurate estimates by each nation of the other's military capabilities. Accuracy of intelligence may be the world's best hope for survival. Clearly, accurate intelligence will become increasingly vital in an age of globalization and an accelerating information technology.

As this is written, ongoing controversies abound about the role and control of secret intelligence. Just as occurred in December 1974, a *New York Times* disclosure in December 2005 of questionable intelligence activities produced a major controversy—and congressional hearings—about the proper limits for spying on Americans in pursuit of strategic information. But in general the public's demand for information, oversight, and accountability will continue to fluctuate, depending on the degree of consensus about security threats and foreign policy goals and programs. In wars people think first about security and then other values. The public's disadvantage is that the intelligence system usually defines the threats.

Meanwhile, the legitimacy of secret intelligence agencies will always be on trial in the absence of all-out war. This may be inevitable, even healthy, for democracy because of the incompatibility of secrecy and accountability.

After extensive hearings, studies and debates, Congress passed the Intelligence Reform and Terrorist Prevention Act of 2004. The act incorporated President George W. Bush's proposals for major restructuring of the national intelligence system and produced the most extensive intelligence reorganization since the CIA's creation by Congress in 1947. In this act the upper-level chairs were rearranged. A new post of Director of National Intelligence (DNI) was created, and the CIA and its director were demoted and charged with the exclusive duties of intelligence collection, analysis, and overseas operations. The DNI was to be the "community" administrator with extensive budgetary and personnel authority. In the process of reform some of the bureaucratic infighting that had occurred prior to the 1947 legislation was evident. At present the real authority of the DNI over sixteen intelligence agencies is uncertain, especially in regard to the role and control of various units of military intelligence. The impact of the 2004 changes will have on more effective accountability remains to be seen. But the new centralized authority offers opportunity for true accountability, which will depend on the aggressive functioning of the major players: the President, Congress, the judiciary, and most important, the press. Above all, effective monitoring and accountability will be a reality only if the President and national intelligence leadership are fully honest and cooperative with the designated congressional watchdogs. Because the requirements of secrecy give the executive the preponderant power, secret intelligence will always put at risk the equilibrium of our constitutional system.

One of the beauties—and perhaps vulnerabilities—of American democracy is that secrets are hard to keep. Undeniably leaks of some very sensitive classified information can do harm. The principle of a free press invites such danger. But an

effective intelligence oversight structure will mitigate that danger. What we don't know can harm us. The challenge is always that of knowing what to do with what we do know.

NOTES

1. Robin Winks, *Cloak and Gown: Scholars in the Secret War* (New York: Morrow, 1987).

2. Harry Howe Ransom, *Central Intelligence and National Security* (Cambridge, MA: Harvard University Press, 1958).

3. See a useful contemporary study of accountability in democratic nations: Hans Born, Loch K. Johnson, and Ian Leigh, *Who's Watching* the *Spies?* (Washington, DC: Potomac Books, 2005).

4. Harry Howe Ransom, "How Intelligent Is Intelligence?," *New York Times Magazine* (May 22, 1960), pp. 26, 80–83.

5. Harry Howe Ransom, "Secret Mission in an Open Society," *New York Times Magazine* (May 21, 1961), pp. 20, 77–79.

6. George P. Schultz, *Turmoil and Triumph; My Years as Secretary of State* (New York: Charles Scribner's Sons, 1993).

APPENDIX A

A SENATE SELECT COMMITTEE ON INTELLIGENCE REPORT ON OVERSIGHT EXPERIENCES, 1947–93

I. EARLY EVOLUTION OF THE U.S. SYSTEM OF OVERSIGHT

OVERSIGHT PRIOR TO 1975

Intelligence activities have been conducted by the United States Government since the beginning of the republic. Historically, these activities were carried out by the departments and agencies responsible for U.S. military and foreign policy. Oversight by the Congress was minimal and devolved to the congressional committees responsible for authorizing or appropriating the budget for the department or agency concerned.

It was not until 1946, in the wake of the Second World War, that President Harry S. Truman, mindful of the surprise attack carried out by the Japanese on Pearl Harbor in 1941, chose to create an intelligence agency, independent of the departments charged with the conduct of foreign relations or the preservation of national defense, to assemble the intelligence available to the government as a whole and provide him with an objective assessment of that information. The Central Intelligence Group, as it was first designated by President Truman, retained many of the operational capabilities of the Office of Strategic Services, which had carried out clandestine intelligence activities during the war. In 1947, as part of the legislation enacted by Congress to establish national defense arrangements in the post-war era, the Central Intelligence Agency (CIA) was created by law, and its Director was given the role of pulling together intelligence obtained by the intelligence elements of other departments and agencies.

Congressional oversight over this new agency was the responsibility of the Committees on Armed Services of the House of Representatives and of the Senate, and appropriations for CIA were handled by the defense subcommittees of the respective

---

Source: "Legislative Oversight of Intelligence Activities: The U.S. Experience," *Report*, S. Prt. 103–88, Select Committee on Intelligence, U.S. Senate, 103d Cong., 2d. Sess. (October 1994), pp. 2–26.

Appropriations Committees of each house of the Congress. The budget for the agency was classified, and, for security reasons, was "buried" in non-descript line-items of the defense budget. (It remains so today.) The bulk of U.S. intelligence activities were, and continue to be, carried out by the Department of Defense. Thus, defense appropriations laws provided an appropriate mechanism for funding intelligence activities.

Congressional awareness of CIA activities was limited largely to the Chairmen and Ranking Minority Members of the committees concerned with the defense budget. Staff involvement was limited generally to one or two senior members of the staff of each of these committees who made certain the needs of the intelligence agencies were funded. Oversight concerns were typically worked out between the Director of Central Intelligence (DCI) and a few congressional participants, with little appreciation by the Congress as a whole and virtually none by the public at large. While there were occasional proposals during the 1950s and 1960s to create special committees with responsibility for intelligence, none of these proposals was adopted by the Congress.

The responsibilities of the DCI evolved over time. It was not until the early 1950s that CIA's responsibility for the conduct of "covert actions" (i.e., efforts to influence the course of events abroad) crystalized. Similarly, CIA did not come into its own as a provider of independent analysis until the Korean War in the early 1950s. In the meantime, new intelligence agencies, such as the National Security Agency and the Defense Intelligence Agency, were created within the Department of Defense, and existing intelligence elements within the military departments, the State Department, and the Federal Bureau of Investigation gradually expanded. DCIs played a relatively weak coordinating role with respect to these agencies, however, until the early 1970s when, at the direction of President Richard M. Nixon, the DCI began to bring together the funding for intelligence activities into a single budgetary program which became formally known as the National Foreign Intelligence Program.

Congressional involvement in these developments remained minimal until the mid-1970s, when a series of especially troubling revelations appeared in the press concerning U.S. intelligence activities. Covert action programs involving assassination attempts against foreign leaders and covert efforts to effect changes in other governments were reported for the first time. The efforts of intelligence agencies to collect information concerning the political activities of U.S. citizens during the late 1960s and early 1970s were also documented extensively by the press.

These programs and practices surprised and concerned many Members of the Senate and House of Representatives. Coming on the heels of the Watergate scandal, which had involved efforts to use and manipulate the CIA and FBI for political purposes, these disclosures suggested to many that intelligence activities, long ignored by the Congress and operated without scrutiny outside the Executive branch, had strayed beyond acceptable limits.

The first legislative response to these disclosures was the enactment in 1974 of the Hughes-Ryan amendment to the Foreign Assistance Act of 1961. This amendment addressed the covert action programs of the CIA, prohibiting the use of appropriated funds for "operations in foreign countries, other than activities intended solely for obtaining necessary intelligence unless and until the President finds that each such operation is important to the national security of the United States." The amendment also required that the President report "in a timely fashion, a description and scope of such operation" to the "appropriate committees of the Congress," which was interpreted to include the Committees

on Armed Services, Foreign Relations (or Foreign Affairs), and Appropriations of each House of Congress, a total of six committees.

The following year, in 1975, Congress passed legislation which, for the fist time, actually terminated funding for a covert operation: the secret support of military and paramilitary activities in Angola.

In the meantime, additional disclosures began to surface in 1975 with regard to the CIA's domestic operations and the efforts of the FBI to undermine the activities of Rev. Martin Luther King and other civil rights leaders during the 1960s. President Gerald Ford reacted to these disclosures by appointing a special commission headed by Vice President Nelson Rockefeller to look into the alleged improprieties, both foreign and domestic. After an investigation of several months, the Rockefeller Commission issued a report in late 1975 that confirmed many of the reported abuses.

Congress was not willing to rely solely upon the findings of the Rockefeller Commission, however, and during 1975 created special investigating committees to investigate the activities of intelligence agencies across the board. The Senate acted first, creating a special committee which became known as the "Church Committee" after the name of its Chairman, Senator Frank Church of Idaho. The House of Representatives followed suit later in the year, creating a similar committee chaired by Congressman Otis Pike of New York.

In the meantime, while the Church and Pike Committee investigations were proceeding, the Ford administration, in February, 1976, issued the first public Executive Order in history to govern intelligence activities—Executive Order 11905. While the new order did not address the obligations of intelligence agencies with respect to the Congress, it did, for the first time, impose restrictions upon intelligence activities, limiting what might be collected by intelligence agencies regarding "U.S. persons" (i.e. citizens, aliens admitted for permanent residence, and organizations predominantly comprised of such persons) and prohibiting U.S. Government employees from engaging in, or conspiring to engage in, political assassinations.

THE CHURCH AND PIKE COMMITTEES (1975–1976)

The Church Committee began its work in January, 1975, and issued a final report, consisting of five volumes, in April, 1976. As a result of voluminous hearings and a series of concurrent investigations directed at virtually every element of the Intelligence Community, the Committee documented a pattern of misconduct on the part of intelligence agencies which, among other things, strongly suggested the need for more effective congressional oversight. The report showed widespread abuse of the civil rights of American citizens and described activities by intelligence agencies that violated applicable law and executive policy, as well as clandestine undertakings in foreign countries which seemed at odds with U.S. values and foreign policy. At the same time, the report made clear that existing legal and policy constraints on intelligence activities were inadequate and that proper supervision and accountability within the Executive branch and to the Congress were sorely lacking.

While the Church Committee made extensive recommendations for change in its final report, it chose not to develop a legislative proposal to address the problems it had documented. Instead, it recommended the Senate create a new follow-on committee to provide continuing oversight and consider such additional legislation as might be necessary. The Pike Committee made a similar recommendation in its final report.

ESTABLISHMENT OF OVERSIGHT COMMITTEES (1976–1977)

On May 19, 1976, after review by five committees and ten days of floor debate, the Senate by a margin of 72–22 voted to create the Select Committee on Intelligence. The resolution creating the new committee—Senate Resolution 400, 94th Congress—remains unchanged and in effect today. (See Appendix, p. 27.) Although established as a "select" committee appointed by the Majority and Minority Leaders of the Senate—a practice normally reserved for committees that serve for a limited period—the Senate Select Committee on Intelligence has continued to function with the support of the body as a whole.

While Senate Resolution 400 did not establish binding legal obligations on the part of intelligence agencies with respect to the new Committee, it did include a non-binding "sense of the Senate" provision stating that the heads of intelligence agencies should keep the Committee "fully and currently informed" of their agency's activities, including "any significant anticipated activities," and provide such information as may be requested by the Committee relating to matters within its jurisdiction.

On July 14, 1977, the House of Representatives created its own oversight committee, by a vote of 227–171. The resolution creating the House committee—House Resolution 658—differed in several respects from its Senate counterpart. Notably, it established the committee as a "Permanent Select Committee on Intelligence," indicating its status as a permanent body under the rules of the House. On the other hand, it did not include the "sense of the Senate" provisions pertaining to the responsibilities of intelligence agencies vis-a-vis the new Committee.

Both committees took the position that they were "appropriate committees" for purposes of receiving notice of covert actions pursuant to the Hughes-Ryan amendment (see above), and this position was acquiesced in by the incoming administration of President Jimmy Carter.

II. STRUCTURE AND OPERATION OF THE OVERSIGHT COMMITTEES

There is no one "right way" to organize legislative oversight of intelligence activities. Indeed, the Senate and House oversight committees are organized differently. The differences reflect both the variation in time—since the Senate committee was the first to be formed and had to overcome more initial resistance—and the difference between the relatively unstructured Senate and the larger House of Representatives, in which rules are followed more rigidly and one political party has had a long period of dominance.

There are, however, some general principles that are worth keeping in mind for any intelligence oversight committee. One is the need to have access to, and to handle properly, very sensitive information on intelligence capabilities and activities. Access to information is the lifeblood of intelligence oversight. Tight security is both an end unto itself and also a means to justify and maintain the committee's access to information. A second need, in many cases, is to limit the role of partisan politics in the operation of the committee. In part, this is one more means of reducing the risk of security lapses that could affect the national security and/or the committee's access to information. It may also serve, however, to

moderate the pace of changes wrought by legislative oversight and thereby to give typically conservative intelligence institutions more time to adjust to a world in which they are accountable to elected representatives of the people.

Key to the effectiveness of the U.S. system has also been control over the budgets of intelligence agencies. As explained below, the oversight committees of the U.S. Congress are involved in funding a myriad of intelligence programs and activities, from large to small. While such a system may not be readily adaptible by other legislatures, some form of budgetary control is essential to encouraging cooperation with the committees responsible for oversight, to obtaining access to information held by intelligence agencies, and generally to encourage compliance with law and direction by the oversight committees.

MEMBERSHIP OF AN OVERSIGHT COMMITTEE

Most committees of the U.S. Senate and House of Representatives distribute their membership in proportion to each political party's membership in that house of congress. Some House committees have been weighted even more strongly in favor of the majority party, however, and occasionally a committee is organized with nearly equal membership for the minority party in order to foster a more bipartisan ethic.

The House intelligence committee's membership has generally been apportioned in the traditional manner, which has given the majority party in the House a substantial majority on the committee as well. By contrast, Senate Resolution 400 apportions the Senate committee's membership in a more bipartisan manner, with the majority party having only a 1-vote margin. The intended effect of that structure, which has been generally borne out in practice, is to limit the ability of any party to count on a bipartisan committee majority to take legislative actions. The need to seek support from members of more than one party, in order to attain a secure majority for legislative action also tends to lessen the likelihood that the committee will approve proposals for radical change.

Both the 19-member House committee and the Senate committee, which has ranged between 13 and 17 members, are structured to include members (at least one from each party) who also serve on each of several other committees that have a legitimate interest in intelligence matters: the Appropriations Committees, the Armed Services Committees, the Judiciary Committees, and the Committees on Foreign Relations (in the Senate) and Foreign Affairs (in the House of Representatives). This membership requirement has almost always been fully implemented, with the result that those related committees have a direct channel of communication with the Intelligence Committees. This has helped to allay the concerns of those committees that the intelligence oversight committees might take (or approve) secret actions that would seriously affect their areas of interest in adverse ways.

Both intelligence committees have limits on the number of years a member may serve before having to leave the committee. The Senate limit is eight years of consecutive service, and the House limit is six years. These limits are designed to ensure a steady rotation of membership, which brings in members with new ideas and approaches, and, over time, to acquaint more members of Congress with this area of government activity.

The selection of members for the Senate committee is also handled in an unusual manner. Most committee memberships are decided by each party's members of the Senate. For the Intelligence Committee, however, members are named by the Majority Leader and the Minority Leader. The intent of this approach is to remove this committee's membership

selection from the normal political process and to permit the leadership of the Senate to select Members whose duties and experience lend themselves to service on the oversight committee.

Each member of the House committee, including members from the minority party, is appointed by the Speaker of the House. Members from the minority party are nominated by the House Minority Leader, and such nominations have heretofore been accepted by the Speaker. The selection process in the House is not specified in the House committee's charter, Rule XLVIII of the Rules of the House, as it is in the resolution creating the Senate Committee.

LEADERSHIP OF AN OVERSIGHT COMMITTEE

As with any legislative committee, there is a premium on strong leadership of an intelligence oversight committee. By and large, the leadership of both the Senate and House committees have been chosen from the members of each party with the longest service on the committee. This serves to maximize the chairman's and vice chairman's familiarity with intelligence oversight, without requiring a background in those agencies.

On rare occasions, an unusual loss of members (through retirements, electoral losses or deaths) and a limit on terms of service on an intelligence oversight committee can result in one party having no experienced members to serve as chairman. Both the Senate and the House of Representatives can handle these or other rare circumstances by agreeing in a particular case not to observe the normal limit on terms of service.

There is often a premium on leadership that reaches across the boundaries of both party and ideology. One organizational measure used by the Senate to foster bipartisanship has been to have the minority party's leading member on the committee serve as vice chairman—and, in the absence of the chairman, as acting chairman—of the committee. Both the chairman and the vice chairman may be substantially deterred from partisan posturing by the knowledge that on any given day, the absence of the chairman may result in a member from the opposition exercising the chairman's powers. This arrangement generally leads to a close working relationship between the chairman and vice chairman, especially in their handling of the most extremely sensitive matters, which may be withheld from other members of the committee.

The House committee has no such formal procedure for shared leadership and has generally been organized on a more partisan basis.

SECURITY

Security is absolutely vital to the operation of an intelligence oversight committee. Although it is also vital for such a committee to have a means of forcing disclosure of information in extremis, day-to-day security is the means by which the committee assures the intelligence agencies—and by which those agencies can assure their sources and co-operative counterparts overseas—that release of information to the committee will not inevitably lead to public disclosure. The experience of the Senate and House committees is that no law or resolution can substitute for the trust that is built upon years of secure handling of sensitive information.

The resolutions establishing each Intelligence Committee provide that classified information and other information received by the committee in confidence may not be

disclosed outside the committee other than in a closed session of the Senate or House of Representatives, respectively, unless the committee votes to release such information and such vote does not prompt an objection from the Executive branch. Failure of members to abide by this restriction subjects them to investigation and, where appropriate, to referral to the Ethics Committee of each House for disciplinary action. In addition, the chairmen of each committee routinely advise their members that anyone who fails to protect such information will be asked to leave the committee. There have, in fact, been instances in which members have left the intelligence committees, either because of an infraction of security rules or because they were unwilling to remain bound by these limits on their actions.

Each committee has the power under its respective charter to release classified information. It must give the President time to object to such disclosure, however, and, if such objection is filed in writing, must vote again on the issue and then take the matter to a closed session of its respective House of Congress, which will make the final determination. In practice, the committees and the Executive branch have reached agreement on disclosures; no President has ever filed a formal objection.

Members of each committee receive access to classified information held by the committee by virtue of their elective office, i.e., they are not subjected to background investigations. Committee staffs, on the other hand, are subjected to background investigations (and reinvestigations) that are carried out by the Federal Bureau of Investigation. (Although a polygraph examination is used as a condition of employment in some intelligence agencies, it is not used with regard to congressional staff appointments.) The results of these investigations are provided to the Committees, who, in turn, seek a "security opinion" from the Director of Central Intelligence (DCI) and Secretary of Defense concerning each potential staff member. While each committee, as a matter of principle, reserves the right to hire its own staff, it is rare that any person is hired for the staff over the objection of the DCI or Secretary of Defense. Indeed, there have been occasional cases in which the committees have declined to hire a potential employee on security grounds despite the absence of objection from the DCI or Secretary of Defense.

Intelligence Committee staff members are required to sign "nondisclosure agreements" pledging not to reveal secret information to which they have access, and they are similarly advised that failure to do so will result in their dismissal. The nondisclosure agreements, by adding a contractual obligation, may open an offending staff member to various civil actions, such as denial of pension rights or recovery of any profits from the improper use of committee information. The agreements also require the pre-publication review (by the committee, which in turn relies upon Executive branch experts) of materials that current or former staff members may wish to publish, unless such materials are clearly unrelated to intelligence matters or the author's service on the committee.

Each committee has established its own security procedures, consistent with (and, in some respects, exceeding) the requirements of the Executive branch. In the Senate committee, the location of each document is controlled every day; all readers of each document are recorded; and there are severe restrictions on the removal of documents from the committee's office spaces or hearing rooms. Thus, if a person attending a closed hearing should take notes, those notes must be surrendered before leaving the room to security staff, who arrange for the secure transportation of the notes to the author's agency. Secure office spaces, including hearing rooms and conference areas, have been constructed for the Intelligence Committees and certified by appropriate security authorities within the Executive branch.

ACCESS TO INFORMATION HELD BY THE INTELLIGENCE COMMUNITY

U.S. intelligence agencies are required by law to furnish to the oversight committees "any information or material concerning intelligence activities . . . which is in their custody or control and which is requested by either of the intelligence committees in order to carry out its authorized responsibilities." The law specifically provides that even information which reveals intelligence sources and methods shall not be denied the committees. In short, the committees, as a matter of law and principle, recognize no limitation on their access to information.

As noted earlier, however, no law can readily compel full access to information if intelligence agencies are convinced that such access will result in catastrophic disclosures of information on their sensitive sources and methods. As a matter of practice, therefore, the committees have been willing to accommodate legitimate concerns for the security of intelligence secrets, either by limiting the scope of their requests or by limiting the manner in which sensitive information is handled, so long as their oversight responsibilities can be fulfilled. Thus, the committees do not ordinarily request the identities of intelligence agents or the details concerning anticipated collection operations where such information is not necessary to the conduct of oversight. Similarly, the committees have refrained from inquiries involving what U.S. intelligence agencies may know about sensitive activities undertaken by their foreign counterparts (other than activities in, or directed at, the United States) where such information is not relevant to the oversight of U.S. agencies. Moreover, the committees have ordinarily been willing to limit access to particularly sensitive information to members and/or a few senior staff, to limit the number of committee members with access to especially sensitive information, or to permit intelligence agencies to retain custody of such information rather than maintaining copies at the committee themselves.

Intelligence agencies typically advise the committees when particularly sensitive information is being requested or provided, and ask that the committees limit the scope of their request or the manner in which such information is to be handled. The committees, for their part, typically satisfy themselves that such requests are legitimate and, once satisfied, negotiate appropriate access or handling arrangements on a case-by-case basis. As a practical matter, instances in which committee access could not be arranged have been extremely rare.

RELATIONS BETWEEN THE CONGRESSIONAL OVERSIGHT COMMITTEES

In general, each of the oversight committees pursues its own agenda during the course of a year in terms of holding hearings, briefings, inquiries, or investigations on subjects of its choosing. Occasionally, events drive both committees to pursue the same objective at the same time and, when this occurs, informal arrangements are often made for both committees to be briefed concurrently, or perhaps for one committee to handle one aspect of an inquiry and for the other to handle a different aspect. Often this will depend upon the level and intensity of member interest in a particular topic.

Generally, it is the practice of intelligence agencies to provide identical information of an oversight nature to the two committees, regardless of which committee actually takes the lead in terms of the inquiry or investigation at issue.

Where the two committees necessarily must come together is over legislation and the annual budget. Because each committee is charged by its respective body with authorizing appropriations for intelligence activities, each year the two committees are responsible for "conferencing" the differences in the annual intelligence authorization bill, as passed by their respective Houses. (The budget process is described in greater detail in the sections that follow.)

While conference on the authorization bill takes place after the bill has cleared each House, typically late in the session, in practice the committees consult quite closely regarding their respective actions on the budget long before conference. Indeed, the committee which reports its bill first may do so based upon its understanding of what the other committee is likely to do when it reports its own version of the bill. The committee which reports its bill last not only has the benefit of seeing what the other committee did, but is able to gauge its own actions in terms of likely trade-offs later in conference.

Both committees must also ultimately agree with respect to any legislation regarding intelligence which may be offered by either committee. Typically, legislative items are included in the public portion of the annual authorization bill (see below), but sometimes they are handled as "freestanding" bills. In either case, since agreement between the two committees will ultimately be required, each committee understands that if it wishes to get legislation enacted, it must ensure not only that the other committee is informed of and appreciates its actions, but also is given an adequate opportunity to examine the legislative initiative in its own process (via hearings or other means) if it chooses to do so. Thus, of necessity, there is close coordination regarding both substance and timing on all legislative initiatives. In practice, this often means that legislation first proposed in one session is not finally enacted until a later session of Congress.

RELATIONS WITH OTHER CONGRESSIONAL COMMITTEES

The resolution establishing the Senate oversight committee provides that the committee will have jurisdiction over the CIA and the "intelligence activities" of other departments and agencies of the Executive branch. The term "intelligence activities" is defined, however, to exclude "tactical foreign military intelligence serving no national policymaking function." The practical effect of these definitions is (1) to leave the CIA and DCI structure within the sole jurisdiction of the intelligence committee; (2) to leave defense intelligence activities other than solely tactical activities to shared jurisdiction between the intelligence and armed services committees; and (3) to leave tactical military intelligence within the sole jurisdiction of the Committee on Armed Services. (Despite this latter limitation, the Senate oversight committee has historically reviewed the annual budget request for tactical military intelligence activities and provided recommendations regarding the request to the Committee on Armed Services.) Standing committees of the Senate whose jurisdiction encompasses departments or agencies which conduct intelligence activities are given the right to seek referral for a period of 30 days of any legislation reported by the Senate intelligence committee pertaining to any matter within the standing committee's jurisdiction. Conversely, the oversight committee is given the right to seek referral for the same period of any legislation reported by other committees which pertains to "intelligence activities" within the jurisdiction of the oversight committee.

A somewhat different arrangement exists in the House of Representatives, where the oversight committee is given jurisdiction over the CIA and the "intelligence *and*

intelligence-related activities" (emphasis added) of other departments and agencies. This term does not exclude "tactical intelligence," and, thus, the House oversight committee retains jurisdiction over this category while the Senate oversight committee does not. Similar provisions apply to the right of other House committees to seek referral of legislation pertaining to matters within their jurisdiction, but the time period for such referral is made a matter of discretion with the Speaker rather than the 30-day period called for by the Senate resolution. The House oversight committee is also authorized to seek referral of legislation covering matters within its jurisdiction which is reported by other committees.

As a practical matter, both oversight committees seek the concurrence of other committees before reporting legislation which contains provisions which might trigger a request for referral. Where concurrence cannot be obtained, the oversight committee has the option of reporting a bill with a provision in dispute (and risking a request for referral or other actions to delay or oppose passage of the bill) or dropping the provision so as to avoid referral.

Both oversight committees also become involved in deliberations concerning legislation in other committees which involve or may affect intelligence agencies. Indeed, intelligence agencies frequently request the assistance of the oversight committees in dealing with legislation in other committees which is believed to adversely affect intelligence operations. The oversight committees typically provide such assistance if they believe a legitimate concern is posed by the legislation under consideration.

Occasionally, the assistance of the oversight committees is sought by other congressional committees. Since other committees often lack staff who are cleared for intelligence matters or otherwise lack the expertise necessary to pursue a particular inquiry, the intelligence committees are asked to conduct investigations or provide their assessments in particular circumstances. For example, an intelligence committee might be asked by its house's Foreign Affairs Committee for an assessment of the behavior of a particular foreign country—based upon information available to intelligence agencies—as part of the Foreign Affairs committee's consideration of legislation to impose sanctions upon the foreign government concerned.

Finally, due to the complex nature of the budget process within the Congress, special coordination occurs between the oversight committees and the respective Armed Services and Appropriations Committees of each House with regard to the annual intelligence authorization. This coordination is explained below in the discussion of the budget process.

RELATIONSHIPS WITH OVERSIGHT MECHANISMS IN THE EXECUTIVE BRANCH

In addition to the oversight provided by the congressional committees, there is an elaborate system of oversight for intelligence activities within the Executive branch. The President's Foreign Intelligence Advisory Board (PFIAB) conducts oversight investigations on an ad hoc basis, reporting its results directly to the President, and requires periodic reports from the Inspectors General at intelligence agencies. Each of the intelligence agencies, in fact, maintains an internal Inspector General who reports to the agency head concerned. Where there are intelligence elements at departments and agencies which are not intelligence agencies per se, e.g., the Department of State, such elements are covered by the Inspector General of the department or agency concerned. The Inspector General at the CIA is appointed by the President and is subject to Senate confirmation, as are the

Inspectors General of departments and agencies which are not intelligence agencies. Inspectors General at other intelligence agencies are typically appointed by the agency head.

The oversight committees have historically had no relationship with the PFIAB, which, as part of the Executive Office of the President, has occupied a privileged status vis-a-vis the Congress under the American system of separation of powers. Nothing prevents elements of the Executive Office of the President and the intelligence committees from cooperating on particular matters, however, where both branches consider it advantageous to do so. For example, the Senate committee contributed to the work of the Vice President's Task Force on Combatting Terrorism in the 1980s.

Moreover, with the exception of the Inspector General at the CIA, there are no formal links between the oversight committees and the Inspectors General at other intelligence agencies. In practice, however, the oversight committees review the activities of the Inspectors General as part of the committees' own oversight responsibilities and occasionally request, via the agency head concerned, that these offices conduct oversight inquiries or investigations in appropriate circumstances and report their results to the oversight committees. The heads of intelligence agencies have historically been responsive to such requests. The CIA Inspector General is required by law to provide reports to the committees on a semi-annual basis and to report "particularly serious or flagrant problems, abuses or deficiencies" within seven days.

In the case of the Inspector General at the CIA, the law creating this office (see Appendix, page 60) also provides that in several unusual circumstances, the Inspector General will report directly to the oversight committees: (1) when the Inspector General is unable to resolve differences with the CIA Director affecting the execution of his or her responsibilities; (2) when the Director or Acting Director is the focus of the Inspector General's activities; and (3) when the Inspector General is unable to obtain significant documentary information in the course of an investigation.

III. FUNCTIONS AND POWERS OF THE OVERSIGHT COMMITTEES

The following sections set forth the functions of the oversight committees. In some cases—particularly where the budget process is concerned—the explanation, while accurate, is somewhat oversimplified in the interests of preserving clarity for the reader with respect to the key points.

AUTHORIZATION OF APPROPRIATIONS FOR INTELLIGENCE: THE BUDGET PROCESS

Both Senate and House resolutions creating the oversight committees empower them to authorize appropriations for intelligence activities. (The House resolution provides for authorization of appropriations for "intelligence and intelligence-related activities.") This means that, consistent with the two-step funding process utilized in the U.S. Congress generally, the oversight committees each year must report legislation to their respective bodies which "authorizes" a certain level of funding for all U.S. intelligence activities. This legislation, in theory, becomes the basis upon which the appropriations committees in each

House then determine how funds are to be appropriated to the department or agency concerned for the next fiscal year (which runs from October 1st until September 30th of each year). Appropriations for intelligence and intelligence-related activities are contained largely in the Department of Defense appropriations bill.

In addition, title V of the National Security Act of 1947 (see Appendix, page 42) provides that intelligence agencies may not spend funds available to them unless they have been both authorized and appropriated. This provision was adopted by Congress in 1985 to ensure that the oversight committees would have a voice in all resource decisions affecting intelligence activities.

Both oversight committees begin with the level of funds requested in the President's budget for intelligence and intelligence-related activities, which typically arrives in February or March of each year. The budget for intelligence activities is contained in the President's National Foreign Intelligence Program (NFIP) budget, which is submitted and justified to the Congress by the Director of Central Intelligence. The budget for "intelligence-related activities" is contained in a budget aggregation known as the Tactical Intelligence and Related Activities (TIARA) budget which is justified by the Secretary of Defense. (Although the Senate committee does not have authorizing authority over TIARA, it receives and analyzes the TIARA budget request and recommends actions on the Administration request to the Committee on Armed Services, which retains authorizing jurisdiction.)

The budget requests for NFIP and TIARA are very detailed funding plans, broken down first into major program categories (e.g., the General Defense Intelligence Program, the National Reconnaissance Program, the Consolidated Cryptologic Program, the FBI Foreign Counterintelligence Program, etc.), and then into specific elements under each major grouping. Specific allocations for both funding and personnel are made for each element. Both budget requests are highly classified.

Once the Administration request has been received, each committee engages in its own elaborate review of the request. These reviews typically are accomplished between February and May of each year and consist of formal hearings, staff visits or briefings, the submission of questions for written response by the agencies, and occasionally in-depth audits or investigations with respect to areas of particular concern to the committee.

On the basis of these reviews, the staffs of each committee formulate recommended positions on the Administration's request which are presented to their respective committees for review, modification, and approval. This takes place in a business meeting of each committee, referred to as the "mark-up" of the annual authorization bill. Typically, the views of the Administration on the proposal are made available to each committee prior to their taking action. Once the committee has "marked up," the bill is formally reported to the parent body, i.e., the House or Senate.

While the authorization bill reported to each parent body is public, the funding and personnel levels being recommended are classified by the Executive branch. The committees deal with this problem by giving legal effect, in the public bill, to a classified "schedule of authorizations" which is incorporated by reference in the public bill and is made available to the Executive branch. Members of the House and Senate are invited to review the schedule at the offices of each committee, but are not provided copies.

The public bill not only authorizes the intelligence budget for the next fiscal year, but also contains numerous legislative measures dealing with such intelligence matters as pension rights, health plans, authority to engage in business activities to provide cover

for intelligence operations, etc. These legislative provisions are further explained in a committee report that, while not carrying the force of law, is still treated both by judges and by the Executive branch as a significant indicator of congressional intent.

There is no secret legislation in the intelligence authorization bill, but the classified "schedule of authorizations" is amplified by a classified report. This report gives the reasons for particular changes that the committee proposes to make in the budget submitted by the President. It also contains direction to the intelligence agencies, ranging from requests for particular studies to direction that particular programs or operations be undertaken, revised, or ended. These provisions are viewed by each committee and understood by the Executive branch to be the basis for the committee's willingness to authorize the intelligence budget. Although as report language they do not carry the force of law, they are generally obeyed by intelligence agencies in order to avoid antagonizing the oversight committees and risking a hostile reaction in the next year's budget cycle.

Once the committees have reported their bills to the floor, they are subject to sequential referral to other committees which have jurisdictional interests in the subject matter of the bill. Historically, in both Houses, the Committee on Armed Services has sought sequential referral of the intelligence authorization bill inasmuch as most of the funding and personnel levels being recommended pertain to elements within the Department of Defense. Other committees may also seek referral should they desire an opportunity to consider specific provisions.

Once the referrals to other committees have been completed, the bills are reported back to the floor by the committee which sought the referral and placed on the calendar for floor action. Historically, this has occurred between June and September of each year. On the floor, the bills are subject to amendment, according to the rules of each House, as is any piece of legislation. Any amendments to the classified "schedule of authorizations" are considered in a closed session of the House concerned, but such amendments have been very rare.

When both Houses have acted on their respective versions of the authorization bill, the body which acted last requests a "conference" with the other body to resolve the differences between the two bills. Typically, all members of the oversight committees in both Houses are appointed as "conferees." Preliminary to a meeting of the conferees, the staffs of both committees develop, where possible, a proposed resolution of the differences in funding between the two bills which is submitted to the conferees for their consideration. Where differences cannot be unresolved in the context of the staff proposal, items of disagreement are placed on the agenda for discussion between conferees. Again, the views of the Administration on the proposed staff resolution and on the issues remaining in dispute are made available to the conferees prior to the conference meeting.

In addition, there is close coordination at this stage with the Appropriations Committees in each House to ensure that the actions of the authorizing committees are generally consistent with those anticipated by the appropriating committees. If the authorizing committees provide authorization where the appropriating committees do not provide appropriations, the authorization is "hollow" or meaningless since funds cannot be spent that have not been appropriated. On the other hand, if the authorizing committees do not provide authorization where the appropriating committees provide appropriated funds, the intelligence agencies are precluded by law from spending the money appropriated. Thus, close coordination with the appropriations committees is essential at this juncture, prior to action by the conferees on the intelligence authorization.

Once agreement has been reached between the conferees, the conference agreement is reported, by a majority vote of the conferees from each House, back to each House for final action. Usually approval of the conference report occurs in September or October of each year, without substantial debate. The conference report contains both the final text of the bill and a "statement of conference managers" that explains the actions taken in conference. The conference report is also accompanied by the final "schedule of authorizations" and a classified explanation, which, like the reports of the individual committees, often contains specific directions to intelligence agencies.

The bill is then enrolled and sent to the President. Once signed, it becomes law. Should the bill be vetoed by the President, a two-thirds vote in each House is required to enact the bill into law.

LEGISLATION

Both oversight committees are legislative committees; that is, they are authorized to have bills within their area of jurisdiction referred to them for disposition and can report legislation to their respective bodies.

Traditionally the oversight committees have used the annual intelligence authorization bill as their primary legislative vehicle, not only for purposes of authorizing appropriations (described above), but also to enact other public law relating to intelligence. The CIA Inspector General Act of 1990, the Intelligence Oversight Act of 1991, and the Intelligence Organization Act of 1992, were each enacted as a separate title to the intelligence authorization bill for the fiscal year concerned. As alluded to above, the committees have also historically used the annual authorization bill to enact administrative authorities needed by intelligence agencies in order to carry out their functions. Indeed, the Administration routinely requests such legislation from the Congress.

Occasionally, the oversight committees have chosen to report "freestanding" bills—outside the context of the annual authorization—where it appears that legislation is needed before the authorization bill can be enacted or where another committee has a significant interest in the legislation, or where the legislation appears so consequential or controversial that the committees believe it preferable to handle such legislation separately. The Foreign Intelligence Surveillance Act of 1978, the Intelligence Identities Protection Act of 1983, and the CIA Voluntary Separation Incentive Act of 1993 were each processed by the committees as separate, "freestanding" bills.

INVESTIGATIONS, AUDITS, AND INQUIRIES

In addition to their legislative functions, the oversight committees are authorized to conduct investigations, audits and inquiries regarding intelligence activities as may be required. These may be prompted by a variety of circumstances: allegations in the news media; confidential communications by employees or former employees of intelligence agencies; or matters that have arisen in the course of the committee's hearings, briefings, or trips.

The committees may also institute investigations or inquiries involving matters that have been reported to the committees through official channels. Such reports come to the committees through a variety of sources. For example, pursuant to various statutes or agreements with Executive agencies, the committees receive periodic reports from the CIA

Inspector General describing his activities; from the Attorney General describing the use of court-ordered electronic surveillance for intelligence purposes; and from the Secretary of Defense advising of the deployment of intelligence assets in particularly sensitive circumstances. Frequently these reports lead to follow-on inquiries and perhaps full-fledged investigations.

Often, these inquiries and investigations involve classified matters which the committees cannot discuss publicly. However, both committees attempt, where possible, to issue public reports where the allegations of improprieties have themselves been public. In recent years, for example, the Senate committee has issued public reports of its investigation into allegations of improper domestic surveillance by the FBI; of its investigation of allegations that CIA may have intentionally withheld pertinent information from a federal court; and of its investigation into allegations that the Reagan White House had improperly withheld documents from the congressional Iran-contra committees.

Generally, the oversight committees refrain from involvement in individual cases unless the facts of a particular case appear to indicate systemic problems or policy shortcomings at the department or agency concerned. And, even here, the committees typically decline involvement when the complainant's case is before the courts or is being considered by the department or agency concerned.

ASSESSING WORLD EVENTS

Although not specifically required by their "charters," both oversight committees attempt to monitor and assess world events where U.S. interests are involved. Typically, this occurs in the form of briefings or hearings where representatives of intelligence agencies testify regarding the significance of these events and respond to questions from the members. In some cases, these briefings involve events which may be the subject of legislation pending before the Congress. Both committees, for example, received numerous briefings by intelligence agencies prior to the votes in each body in 1991 to commit U.S. armed forces to the liberation of Kuwait.

In some cases, the committees look back on events that have already taken place to assess the value of the intelligence support to U.S. policymakers or military commanders. Such assessments took place, for example, in both committees after the U.S. actions in Panama in 1989 and in Kuwait in 1991.

By making these assessments, the committees are able to test and evaluate the quality and timeliness of the intelligence analysis performed by elements of the Intelligence Community and come to understand the strengths and shortcomings of U.S. intelligence-gathering capabilities. This, in turn, affects the committees' respective actions on the budget and may suggest legislative initiatives as well.

CONFIRMATION OF PRESIDENTIAL APPOINTEES

Under the U.S. Constitution, certain Government officers are appointed by the President, "by and with the advice and consent of the Senate." Such positions include the Director of Central Intelligence, the Deputy Director of Central Intelligence, and the CIA Inspector General. In the Senate, the Select Committee on Intelligence reviews the nominations of individuals appointed to these positions.

The Senate Committee routinely explores the background of all nominees to assess the fitness of the nominee concerned as well as to identify possible conflicts of interest. It routinely investigates all allegations of improper conduct which might be made regarding the nominee either in the press or to the committee privately. The Chairman and Vice Chairman of the Committee are also provided access to the background investigation performed on the nominee by the FBI.

Public hearings are then conducted on the nomination where the nominee and others who have pertinent information to share regarding the nominee testify before the Committee. Depending upon the circumstances, these hearings have been the occasion for in-depth inquiries into events of the past, as in the Robert Gates confirmation hearings in 1991, and typically provide an opportunity to learn the nominee's vision of the future, as was the case with the R. James Woolsey confirmation hearing in 1993.

In either event, the Senate committee has traditionally used these occasions not only to ascertain the views of the nominee with regard to intelligence, but also to obtain commitments from nominees towards the oversight process itself. Confirmation hearings not only serve to acquaint the Senate committee with the leaders of the Intelligence Community with whom it must closely work, but also to inform the nominee with respect to the views and concerns of the committee itself.

CONSIDERATION OF TREATIES

Under the U.S. Constitution, the President may ratify a treaty only if the Senate has consented to it. While treaties are typically referred to the Senate Committee on Foreign Relations, the Select Committee on Intelligence is routinely asked to evaluate arms control treaties and other similar agreements where the ability of the United States to determine violations by the other signatories is an issue for the Senate as a whole.

Typically, the Senate committee holds extensive hearings on the verification aspects of such treaties, and issues both classified and unclassified reports regarding its findings and recommendations. Such reports were issued with regard to the ability of the United States to verify the SALT II treaty in 1979; the INF treaty in 1988; the Threshold Test Ban Treaty and Treaty on Peaceful Nuclear Explosions in 1990; the CFE treaty in 1991; the START treaty in 1992; and the Open Skies treaty in 1993. The findings and recommendations contained in these reports are, in turn, ordinarily addressed in the reports issued by the Committee on Foreign Relations regarding the treaties themselves.

IV. OVERSIGHT IN PRACTICE: (1977–1995)

OVERSIGHT DURING THE CARTER ADMINISTRATION (1977–1980)

Coming to office on the heels of the Church and Pike Committee investigations, the Carter Administration sought to establish a clear legal framework for U.S. intelligence activities by working at two levels: first, by drafting a new Executive Order on intelligence activities; and second, in consultation with the two newly-formed congressional oversight committees, by developing legislation to establish in law the mission and functions of U.S. intelligence agencies.

Among the most important provisions of the new Executive order—Executive Order 12036 of January 26, 1978—was a requirement that the restrictions on intelligence-gathering contained in the order be implemented in regulations of each intelligence agency that would have to be approved by the Attorney General. This not only ensured consistency in approach throughout the Intelligence Community but also provided legal review external to intelligence agencies of the rules governing their activities.

Executive Order 12036 also, for the first time, directed the Director of Central Intelligence and the heads of intelligence agencies to keep the two congressional intelligence committees "fully and currently informed" of intelligence activities, including "significant anticipated activities," and to provide pertinent information in their possession to the oversight committees—subject to the constitutional authorities of the President and the statutory duty of the Director of Central Intelligence to protect intelligence sources and methods. This was the first binding direction to intelligence agencies to cooperate with their congressional oversight committees.

The effort to craft "charter legislation" for U.S. intelligence agencies did not fare so well. In 1978, the Senate committee introduced a detailed bill which not only set forth missions and functions for each agency, but also proposed complex restrictions and limitations upon the operations of each agency. After months of consultation and after ever-increasing objections from the intelligence agencies that the proposed restrictions would hamper them in accomplishing their missions, the Carter Administration eventually abandoned its effort to develop a bill agreeable to both itself and Congress, preferring instead to rely upon the new Executive order to provide the fundamentals of control.

Unable to reach agreement with the Administration on the "missions and functions" portion of the legislation, and deeply concerned over the Administration's failure to inform them of intelligence operations relating to the failed attempt to rescue U.S. hostages in Iran, the oversight committees turned their attention to the portion of the bill that would establish the legal obligations of intelligence agencies towards the two oversight committees. Months of negotiation eventually resulted in an agreement between the oversight committees and the Administration, ultimately enacted into law as Title V of the National Security Act of 1947, also known as "the Intelligence Oversight Act of 1980." (See appendix, p. 42.) Significantly, this legislation established as a matter of law (consistent with the constitutional responsibilities of the President) the obligation of intelligence agencies—

To keep the congressional intelligence committees "fully and currently informed";

To report "significant anticipated intelligence activities" to the committees;

To provide prior notice of covert actions to the committees and, where prior notice could not be provided, to provide notice "in a timely fashion"; and

To report violations of law and "significant intelligence failures" to the committees "in a timely fashion."

In return for the Administration's agreement to make the obligations of intelligence agencies to the oversight committees a matter of law, the Hughes-Ryan amendment was changed to require notice of covert actions only to the two intelligence committees (i.e., the legal requirement to notify six other committees was eliminated).

During this period, the committees continued to consolidate their positions within their respective bodies. In 1977, the Senate committee, with the agreement of the Committee on

Armed Services, assumed responsibility for reviewing presidential nominations of the Director and Deputy Director of Central Intelligence. In 1978, the committees produced the first bill authorizing appropriations for intelligence activities ever enacted by the Congress. (Previously, appropriations for intelligence were drawn from defense appropriations without systematic congressional review of intelligence activities.) Both committees held public hearings during this period on the issue of whether the dollar figure for the total intelligence budget should be made public. Investigations and inquiries were conducted by both bodies. While confusion with respect to the obligation of intelligence agencies to provide information to the committees remained considerable—notwithstanding the new 1980 law—it did not prevent either committee from carrying out investigations requiring access to highly sensitive information.

The committees also played a major role during this period in the enactment of legislation related to intelligence. Acting in concert with the Judiciary Committees in each House, the committees developed legislation known as the Foreign Intelligence Surveillance Act of 1978 (see appendix p. 65) which, for the first time, required that a court order be obtained from a special court established under the Act as a condition for undertaking electronic surveillances for intelligence purposes within the United States. Heretofore, such surveillances had been carried out without a search warrant or court order, pursuant to the asserted constitutional authority of the President. The committees were also instrumental in the enactment of the Classified Information Procedures Act of 1980, which established statutory procedures for handling classified information involved in a federal criminal proceeding. The law provided an in camera process for determining the relevance of classified information that a defendant might wish to use at trial and required federal judges to consider a variety of alternatives to protect national security information from being publicly disclosed during a criminal trial, rather than posing an "all or nothing" dilemma for the Government, i.e., reveal a secret or give up a prosecution.

OVERSIGHT DURING THE REAGAN ADMINISTRATION (1981–1988)

The Reagan Administration came to office with the express intent of reducing where appropriate the bureaucratic constraints placed upon intelligence agencies and increasing the level of resources available to these agencies, which had been sharply reduced during the 1970s.

It began by revising the Carter Executive order on intelligence, issuing Executive Order 12333 (see Appendix, p. 87) on December 4, 1981. The specific obligations of intelligence agencies contained in the Carter order pertaining to congressional oversight were replaced simply by a reference to the new oversight statute enacted the year before (see above). The new Administration also requested increased resources for intelligence, and these requests were generally supported by the oversight committees.

The new Administration also brought in a controversial Director of Central Intelligence, William J. Casey, and, for the first time, the oversight committees—particularly the Senate committee—took an aggressive role in investigating allegations concerning a sitting Director. Although DCI Casey had only recently been confirmed, the Select Committee on Intelligence opened an intensive investigation of allegations of improper conduct on the part of the new Director while he had been in the private sector, concluding that Casey was "not unfit to serve" as head of the CIA.

During the first Reagan Administration, new legislation—favorable to intelligence agencies—was enacted. In 1982, the Intelligence Identities Protection Act became law, making it a crime to reveal the identity of intelligence agents under certain circumstances. In 1984, the Central Intelligence Agency Information Act was passed, exempting certain CIA operational files from being searched in response to requests received by CIA under the Freedom of Information Act. The committees also looked closely at the implementation of the Foreign Intelligence Surveillance Act to assure themselves and the public that it was being administered properly.

During this period, the oversight committees became increasingly concerned with the role of U.S. intelligence agencies in Central America. Investigations were conducted into allegations that CIA may have been involved in political violence in El Salvador and Guatemala. Yet the issue which clearly caused the greatest concern was the CIA's role in the civil war taking place in Nicaragua. In one highly publicized incident which occurred in 1984, the Chairman and Vice-Chairman of the Senate Committee, Senators Goldwater and Moynihan, respectively, severely chastized Director Casey for failing to advise the Committee that CIA had participated in mining a harbor in Nicaragua. This led to renewed discussions with the Administration in terms of keeping the Committees "fully and currently informed" of developments in covert action operations which had previously been briefed to the Committees. Ultimately, an informal agreement, referred to as "the Casey Accords," was agreed to which provided that "memoranda of notification" would be provided the oversight committees to advise them of significant changes or developments in ongoing covert operations.

The committees also became increasingly involved during this period in congressional efforts to limit U.S. assistance to the Nicaraguan rebels. A series of funding restrictions—known collectively as the "Boland Amendments" (after the name of the original sponsor of the first such restriction, Congressman Edward Boland, Chairman of the House Permanent Select Committee on Intelligence)—placed limits on U.S. assistance by both intelligence and military elements of the U.S. Government and were enacted as part of annual authorization or appropriation bills.

Alarmed by a spate of serious espionage cases in 1985 and 1986 (e.g., the Walker-Whitworth case, the Pelton case, and Pollard case), both committees also undertook extensive reviews of U.S. counterintelligence and security policies and practices during this time period.

The second Reagan Administration produced what the committees regarded as the most serious breach of the oversight arrangements since the committees were created: the so-called Iran-contra affair. In November, 1986, the oversight committees learned for the first time that the President had approved a covert action finding ten months earlier authorizing the sale of arms to Iran in an effort to obtain the release of American hostages being held in Lebanon and had specifically ordered that the oversight committees not be notified. The committees also learned that Administration officials had used the proceeds of these sales to provide assistance to the Nicaraguan rebels at a time when the use of appropriated funds for such purpose was prohibited by law. It also came to light that certain officials in the Administration had entertained the idea of funding covert action programs with funds other than those which had been authorized and appropriated by the Congress, avoiding the congressional oversight process altogether. Both committees undertook intensive investigations of these events during November-December, 1986. These inquiries were followed by the appointment of special investigating committees in each House in January, 1987.

While the Iran-contra investigation was proceeding, both committees sought to shore up the existing oversight arrangements in light of what they had learned. While the Reagan Administration adopted new procedures recommitting itself to the oversight arrangements, bills were introduced in both Houses calling for notice to the committees of all covert actions within 48 hours of their approval without exception, and hearings were held on the bills in the fall of 1987.

In the meantime, with DCI Casey incapacitated by illness, the Administration nominated Deputy DCI Robert M. Gates to be the new Director in February, 1987. After a series of confirmation hearings by the Senate committee which highlighted the role of the nominee in the Iran-contra affair—then under investigation by the special investigating committee and by a special prosecutor—Gates asked that his nomination be withdrawn. The Administration then nominated Judge William H. Webster, who was then serving as Director of the FBI, to be the new Director of Central Intelligence. A second round of confirmation hearings ensued with Webster ultimately being confirmed by the Senate in May, 1987, after pledging to restore the trust and cooperative working relationship shattered by the Iran-contra affair.

Subsequently, the work of the special investigating committees ended and in October, 1987, the final report of the committees was issued, endorsing, among other things, the 48-hour bills then pending.

In the spring of 1988, the Senate passed a bill requiring 48-hour notice of covert actions by a vote of 71–19, but no action was taken in the House. The 48-hour bill thus died without being enacted, at a time when a new Administration was coming into office.

In the summer of 1988, the Senate committee undertook an extensive oversight inquiry into the FBI's investigation of a domestic political group, the Committee in Solidarity with the People of El Salvador (CISPES) during the early 1980s, finding several violations of existing guidelines for such investigations. As a result of this and an internal inquiry conducted by the FBI Inspection Division, six FBI agents were disciplined by the Director of the FBI.

OVERSIGHT DURING THE BUSH ADMINISTRATION (1989–1992)

Met with pledges of commitment to the oversight process from the incoming Administration, the intelligence committees did not immediately press for enactment of the 48-hour bill, but sought instead to obtain a formal, written explanation from the new President with respect to how he intended to implement the statutory requirement to provide notice of covert actions "in a timely fashion." After several months of discussion, President Bush wrote to the oversight committees in October, 1989, saying that he would ordinarily provide prior notice of covert actions to the committees, but where that was not possible, he would provide notice "within a few days." Should notice be withheld for a longer period, the President stated, he would rely upon his authorities under the Constitution. In its version of the intelligence authorization bill for fiscal year 1990, the Senate adopted language which would have incorporated this formulation into the oversight statute itself, but this language was dropped from the bill in conference after the House committee disagreed with this proposal.

The oversight committees were able to agree, however, on one proposal growing out of the Iran-contra affair by including in the fiscal year 1990 intelligence authorization bill a provision calling for the creation of an independent Inspector General at the Central

Intelligence Agency appointed by the President rather than the Director with responsibilities to report directly to the oversight committees under certain circumstances. (See Appendix, p. 60.) This legislation marked the first time Congress had created by law an oversight mechanism within an intelligence agency.

During 1990, both committees renewed their efforts to modify the oversight statute to incorporate the understandings they believed had been reached with the President in terms of reporting covert actions to the Congress and to deal with other problems which had surfaced in the course of the Iran-contra affair. Relying upon informal assurances from senior Administration officials that the proposed language on these points was agreeable, the committees adopted language in the intelligence authorization bill for fiscal year 1991 which included a substantial revision of the Intelligence Oversight Act of 1980. The Administration subsequently had second thoughts regarding the proposed legislation and, after Congress had adjourned for the year, the President vetoed the bill.

This action led to further negotiations during the early part of 1991 to resolve the concerns of the Administration, and, after months of negotiation, a compromise was finally achieved, allowing for passage of the fiscal year 1991 intelligence authorization bill in August, 1991. (See Appendix, p. 42.) The bill revised the Intelligence Oversight Act of 1980 in its entirety and, among other things, provided that:

> Presidential approvals of covert actions must be in writing and cannot retroactively authorize such actions;
>
> Reports to the Congress must identify all government entities participating in the operation and state whether third parties outside of government control are involved;
>
> Covert actions cannot not be used to influence U.S. politics or domestic opinion;
>
> Covert actions cannot violate the laws of the United States or the U.S. Constitution; and
>
> Significant changes to ongoing operations must be approved by the President and reported to the committees in the same manner as the original operation.

Insofar as the longstanding issue of "timely" notice was concerned, the compromise left intact the existing statutory formulation requiring prior notice ordinarily and, where that is not possible, requiring notice "in a timely fashion." But for the first time, report language was included which said that the committees interpreted the phrase "in a timely fashion" as meaning "within a few days," consistent with the position previously taken by the President. While the report acknowledged that the President may assert authority under the Constitution to withhold for longer periods, the committees expressed the view that the Constitution did not provide such authority to the President. The issue was left at this philosophical impasse.

While the negotiations over the changes to the oversight statute were taking place during the summer of 1991, DCI Webster resigned, and the President nominated Robert M. Gates, whose nomination had been withdrawn four years earlier, to replace him. The Senate Committee held extensive hearings regarding the nomination, focusing particularly on the role of Gates in the Iran-contra affair and on allegations that he had slanted intelligence analysis at the CIA to conform to a particular political viewpoint. Indeed, the Gates hearings constituted the first in-depth exploration of the intelligence analytical process which had ever taken place in a public forum.

Despite the controversial nature of the hearings themselves, the Committee voted 11–4 to report the nomination, and Gates was confirmed by the Senate by a vote of 64–31 in October, 1991.

The new DCI immediately undertook an extensive reexamination of the role of the Intelligence Community in the post-Cold War era. The committees, for their part, followed suit. In January, 1992, the chairmen of both committees introduced far-reaching bills to reorganize the Intelligence Community, and extensive hearings on the legislation were undertaken by both bodies.

In the fall of 1992, after several months of negotiation between the Administration and the oversight committees, agreement was reached on "The Intelligence Organization Act of 1992," which amended the National Security Act of 1947 to provide explicitly for the responsibilities and authorities of the Director of Central Intelligence. (See Appendix, page 48.) Although the new law did not, as a practical matter, represent a radical departure from the status quo, it did represent a substantial change in the legal framework for U.S. intelligence activities. Among other things, the new law:

Recognized the role of the DCI as statutory advisor to the National Security Council;

Recognized the three roles of the DCI as (1) principal intelligence advisor to the President, (2) head of the U.S. Intelligence Community, and (3) head of the CIA;

Established in law the National Intelligence Council as the highest authority for developing and publishing intelligence analysis;

Gave the DCI responsibility for establishing priorities for U.S. Government intelligence-gathering and for coordinating all collection involving human sources, both overt and clandestine;

Gave the DCI authority to approve the budgets of intelligence agencies and provided that once approved, funds could not be reprogrammed to other purposes without the approval of the DCI; and

For the first time in statute, defined the term "Intelligence Community."

Indeed, the new law represented the first successful effort by the Congress to enact organizational legislation for the U.S. Intelligence Community since 1947.

In the fall of 1992, both committees undertook extensive investigations into allegations that CIA had provided false or misleading information to a federal criminal proceeding in Atlanta, Georgia, involving a branch manager of the Banca Nazionale Del Lavoro (BNL), headquartered in Rome, Italy. The Senate committee produced a lengthy report of its inquiry contained numerous recommendations for improving the relationship between intelligence agencies and law enforcement authorities.

OVERSIGHT IN THE CLINTON ADMINISTRATION (1993–)

The Clinton administration has continued the commitment to the congressional oversight process, but has as of this writing (mid-1994) undertaken no significant organizational or structural change within the Intelligence Community.

In 1993, freestanding legislation was enacted permitting the Director of Central Intelligence to offer financial incentives to senior employees to retire at an earlier date, in an effort to assist the CIA in meeting its manpower reduction objectives.

In 1994, in the wake of the arrest of a CIA employee and his wife for espionage, both committees conducted oversight inquiries into CIA security practices and reported legislative proposals to improve the U.S. counterintelligence and security posture. Supported by the Clinton administration, certain of the legislative proposals were enacted as part of the intelligence authorization bill for fiscal year 1995.

In particular, legislation was enacted to expand the Foreign Intelligence Surveillance Act to impose the same court order procedure to authorize physical searches for intelligence purposes as had existed for electronic surveillances since 1978. The legislation also contained provisions requiring improved coordination of counterintelligence matters with the FBI and provisions to enhance the investigative authorities of federal counterintelligence agencies.

The Congress also enacted legislation to create a new commission to review the roles and missions of U.S. intelligence agencies in the post-Cold War era, and charged it with producing a report to the President and the Congress by March 1, 1996. In essence, the commission was asked to reexamine the basic assumptions underlying the intelligence function. It was envisioned that this review, once completed, would provide the basis for subsequent actions by the intelligence committees for years to come.

APPENDIX B

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

Editor's note: Congress passed another important intelligence oversight bill in between the Hughes-Ryan Act of 1974 (with its attention to covert action) and the Intelligence Oversight Act of 1980 (with its concern for prior notification about all significant foreign intelligence operations). It was called the Foreign Intelligence Surveillance Act—FISA, for short—and it set up a special court where the intelligence agencies or the White House could go to obtain a warrant for electronic or other forms of surveillance against suspected terrorists or other threats to the nation. The FISA warrant procedure became controversial in 2004 when the *New York Times* reported that the second Bush administration had been using the National Security Agency for electronic surveillance against terrorist suspects without first acquiring a warrant, as required by FISA. The language of the law is reprinted in this appendix.

FOREIGN INTELLIGENCE SURVEILLANCE

Section

§ 1801. Definitions

As used in this title [50 USCS §§ 1801 et seq]:

(a) "Foreign power" means—

(1) a foreign government or any component thereof whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons; or

(6) an entity that is directed and controlled by a foreign government or governments.

(b) "Agent of a foreign power" means—

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statues of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; or

(D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(c) "International terrorism" means activities that—

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended—

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(d) "Sabotage" means activities that involve a violation of chapter 105 of title 18, United States Code, [18 USCS §§ 2151 et seq.], or that would involve such a violation if committed against the United States.

(e) "Foreign intelligence information" means—

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(f) "Electronic surveillance" means—

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) "Attorney General" means the Attorney General of the United States (or Acting Attorney General) or the Deputy Attorney General.

(h) "Minimization procedures," with respect to electronic surveillance, means—

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a) [50 USCS § 1802(a)], procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 105 [50 USCS § 1805] is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act [8 USCS § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

(j) "United States," when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) "Contents," when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

(o) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.

(Oct. 25, 1978, P. L. 95–511, Title I, § 101, 92 Stat. 1783.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Short titles:

Act Oct. 25, 1978, P. L. 95–511, § 1, 92 Stat. 1783, provided: "this Act [50 USCS §§ 1801 et seq., generally; for full classification of this Act, Consult USCS Tables volumes] may be cited as the 'Foreign Intelligence Surveillance Act of 1978'.".

Other provisions:

Effective date of Act Oct. 25, 1978; exception. Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided: "The provisions of this Act [50 USCS §§ 1801 et seq., generally; for full classification of the Act, consult USCS Tables volumes] and the amendments made hereby shall become effective upon the date of enactment of this Act [enacted Oct. 25, 1978], except that any electronic surveillance approved by the Attorney General to gather foreign intelligence information shall not be deemed unlawful for failure to follow the procedures of this Act, if that surveillance is terminated or an order approving that surveillance is obtained under title I of this Act [50 USCS §§ 1801 et seq.] within ninety days following the designation of the first judge pursuant to section 103 of this Act [50 USCS § 1803]."

RESEARCH GUIDE

Law Review Articles:

Shapiro, Foreign Intelligence Surveillance Act: Legislative Balancing of National Security and the Fourth Amendment. 15 Harvard Journal of Legislation 119, December, 1977.

United States v Butenko (494 F2d 593): Executive Authority to Conduct Warrantless Wiretaps for Foreign Security Purposes. 27 Hastings L J 705, January, 1976.

Nesson, Aspects of the Executive's Power Over National Security Matters: Secrecy Classifications and Foreign Intelligence Wiretaps. 49 Ind L J 399, Spring, 1974.

Wiretapping of an Alien Spy for Foreign Intelligence Purposes Does not Violate Communications Act of 1934 or Fourth Amendment. 8 NYU Journal of International Law and Politics 479, Winter, 1976.

Present and Proposed Standards for Foreign Intelligence Electronic Surveillance. 71 Northwestern L Rev 109, March-April, 1976.

Presidential Power to Conduct Electronic Surveillance for Foreign Affairs Purposes. 20 Villanova L Rev 833, March, 1975.

Fourth Amendment and Executive Authorization of Warrantless Foreign Security Surveillance. 1976 Washington U L Q 397, Spring, 1978.

Fourth Amendment and Judicial Review of Foreign Intelligence Wiretapping: Zweibon v. Mitchell (516 F2d 594). 45 George Washington L Rev 55, November, 1976.

§ 1802. Electronic surveillance authorization without court order; certification by Attorney General; reports to congressional committees; transmittal under seal; duties and compensation of communication common carrier; applications; jurisdiction of court

(a) (1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title [50 USCS §§ 1801 et seq.] to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—

(A) the electronic surveillance is solely directed at—

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 101(a) (1), (2), or (3) [50 USCS § 1801(a)(1), (2), or (3)]; or

(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 101(a) (1), (2), or (3) [50 USCS § 1801(a)(1), (2), or (3)];

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h) [50 USCS § 1801(h)]; and

if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 108(a) [50 USCS § 1808(a)].

(3) The Attorney General shall immediately transmit under seal to the court established under section 103(a) [50 USCS § 1803(a)] a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of Central Intelligence, and shall remain sealed unless—

(A) an application for a court order with respect to the surveillance is made under sections 101(h)(4) and 104 [50 USCS §§ 1801(h)(4) and 1804]; or

(B) the certification is necessary to determine the legality of the surveillance under section 106(f) [50 USCS § 1806(f)].

(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to—

(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and

(B) maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid.

(b) Applications for a court order under this title [50 USCS §§ 1801 et seq.] are authorized if the President has, by written authorization, empowered the Attorny [Attorney] General to approve applications to the court having jurisdiction under section 103 [50 USCS § 1803] and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 105 [50 USCS § 1805], approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) unless such surveillance may involve the acquisition of communications of any United States person.

(Oct. 25, 1978, P. L. 95–511, Title I, § 102, 92 Stat. 1786.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Explanatory notes:

The bracketed word "Attorney" was inserted in subsec. (b) to denote word probably intended by Congress.

Effective date of section:

Act Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided that this section is generally effective on Oct. 25, 1978. For exception, see note containing Act Oct. 25, 1978, § 301, located at 50 USCS § 1801.

Other provisions:

Foreign intelligence electronic surveillance. Ex. Or. No. 12139 of May 23, 1979, 44 Fed. Reg. 30311, provided:

"1-101. Pursuant to Section 102(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1802(a)) [subsec. (a)(1) of this section], the Attorney General is authorized to approve electronic surveillance to acquire foreign intelligence information without a court order, but only if the Attorney General makes the certifications required by that Section.

"1-102. Pursuant to Section 102(b) of the Foreign Intelligence Act of 1978 (50 U.S.C. 1802(b)) [subsec. (b) of this section], the Attorney General is authorized to approve applications to the court having jurisdiction under Section 103 of that Act [50 USCS § 1803] to obtain orders for electronic surveillance for the purpose of obtaining foreign intelligence information.

"1-103. Pursuant to Section 104(a)(7) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804(a)(7)) [50 USCS § 1804(a)(7)], the following officials, each of whom is employed in the area of national security or defense, is designated to make the certifications required by Section 104(a)(7) of the Act in support of applications to conduct electronic surveillance:

"(a) Secretary of State.

"(b) Secretary of Defense.

"(c) Director of Central Intelligence.

"(d) Director of the Federal Bureau of Investigation.

"(e) Deputy Secretary of State.

"(f) Deputy Secretary of Defense.

"(g) Deputy Director of Central Intelligence.

"None of the above officials, nor anyone officially acting in that capacity, may exercise the authority to make the above certifications, unless that official has been appointed by the President with the advice and consent of the Senate.

"1-104. Section 2–202 of Executive Order No. 12036 is amended by inserting the following at the end of that section: 'Any electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act as well as this Order.'.

"1-105. Section 2–203 of Executive Order No. 12036 is amended by inserting the following at the end of that section: 'Any monitoring which constitutes electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978 shall be conducted in accordance with that Act as well as this Order.' "

§ 1803. Designation of judges

(a) Court to hear applications and grant orders; record of denial; transmittal to court of review. The Chief Justice of the United States shall publicly designate seven district court judges from seven of the United States judicial circuits who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Act, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this Act which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this Act, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b).

(b) Court of review; record, transmittal to Supreme Court. The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the

presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this Act. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(c) Expeditious conduct of proceedings; security measures for maintenance of records. Proceedings under this Act shall be conducted as expeditiously as possible. The record of proceedings under this Act, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence.

(d) Tenure. Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) shall be designated for terms of three, five, and seven years.(Oct. 27, 1978, P. L. 95–511, Title I, § 103, 92 Stat. 1788.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

References in text:

"This Act," referred to in this section, is Act Oct. 25, 1978, P. L. 95–511, 92 Stat. 1783, popularly known as the Foreign Intelligence Surveillance Act of 1978, which is generally classified to 50 USCS §§ 1801 et seq. For full classification of this Act, consult USCS Tables volumes.

Effective date of section:

Act Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided that this section is generally effective on Oct. 25, 1978. For exception, see note containing Act Oct. 25, 1978, § 301, located at 50 USCS § 1801.

§ 1804. Applications for court orders

(a) Submission by Federal officer; approval of Attorney General; contents. Each application for an order approving electronic surveillance under this title [50 USCS §§ 1801 et seq.] shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 103 [50 USCS § 1803]. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this title [50 USCS §§ 1801 et seq.]. It shall include—

(1) the identity of the Federal officer making the application;

(2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;

(3) the identity, if known, or a description of the target of the electronic surveillance;

(4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(5) a statement of the proposed minimization procedures;

(6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate—

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that the purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e) [50 USCS § 1801(e)]; and

(E) including a statement of the basis for the certification that—

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques;

(8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(9) a statement of the facts concerning all previous applications that have been made to any judge under this title [50 USCS §§ 1801 et seq.] involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;

(10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this title [50 USCS §§ 1801 et seq.] should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and

(11) whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

(b) Exclusion of certain information respecting foreign power targets. Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a)(1), (2), or (3) [50 USCS § 1801(a)(1), (2) or (3)], and each of the facilities or places at which the surveillance is directed is owned, leased, exclusively used by that foreign power, the application need not contain the information required by paragraphs (6), (7)(E), (8), and (11) of subsection (a) [50 USCS § 1801(a)(6), (7)(E), (8) and (11)], but shall state whether physical entry is required to effect the surveillance and shall contain such information about the surveillance techniques and communications or other information

concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.

(c) Additional affidavits or certifications. The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(d) Additional information. The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105 [50 USCS § 1805].

(Oct. 25, 1978, P. L. 95–511, Title I, § 104, 92 Stat. 1788.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Effective date of section:

Act Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided that this section is generally effective on Oct. 25, 1978. For exception, see note containing Act Oct. 25, 1978, § 301, located at 50 USCS § 1801.

Other provisions:

Foreign intelligence electronic surveillance. For provisions governing electronic surveillance to acquire foreign intelligence information, see Ex. Or. No. 12139 of May 23, 1979, 44 Fed. Reg. 30311, located at 50 USCS § 1802 note.

§ 1805. Issuance of order

(a) Necessary findings. Upon an application made pursuant to section 104 [50 USCS § 1804], the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—

(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;

(2) the application has been made by a Federal officer and approved by the Attorney General;

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the electronic surveillance is a foreign power or agent of a foreign power: *Provided,* That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) the proposed minimization procedures meet the definition of minimization procedures under section 101(h) [50 USCS § 1804(h)]; and

(5) the application which has been filed contains all statements and certifications required by section 104 [50 USCS § 1804] and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 104(a)(7)(E) [50 USCS § 1804(a)(7)(E)] and any other information furnished under section 104(d) [50 USCS § 1804(d)].

(b) Specifications and directions of orders. An order approving an electronic surveillance under this section shall—

(1) specify—

(A) the identity, if known, or a description of the target of the electronic surveillance;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;

(E) the period of time during which the electronic surveillance is approved; and

(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device; and

(2) direct—

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(c) Exclusion of certain information respecting foreign power targets. Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a)(1), (2), or (3) [50 USCS § 1801(a)(1)(2), or (3)], and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order need not contain the information required by subparagraphs (C), (D), and (F) of subsection (b)(1) [50 USCS § 1801(b)(1)(C), (D), and (F)], but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.

(d) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated. (1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 101(a)(1), (2), or (3) [50 USCS § 1801(a)(1), (2) or (3)], for the period specified in the application or for one year, whichever is less.

(2) Extensions of an order issued under this title [50 USCS §§ 1801 et seq.], may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except

that an extension of an order under this Act for a surveillance targeted against a foreign power, as defined in section 101(a)(5) or (6) [50 USCS § 1801(a)(5) or (6)], or against a foreign power as defined in section 101(a)(4) [50 USCS § 1801(a)(4)] that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e) Emergency orders. Notwithstanding any other provision of this title [50 USCS §§ 1801 et seq.], when the Attorney General reasonably determines that—

(1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and

(2) the factual basis for issuance of an order under this title [50 USCS §§ 1801 et seq.] to approve such surveillance exists;

he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 103 [50 USCS § 1803] is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this title [50 USCS §§ 1801 et seq.] is made to that judge as soon as practicable, but no more than twenty-four hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this title [50 USCS §§ 1801 et seq.] for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of twenty-four hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 103 [50 USCS § 1803].

(f) Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel. Notwithstanding any other provision of this title [50 USCS §§ 1801 et seq.], officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance

not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

(1) test the capability of electronic equipment, if—

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and:

(D) *Provided,* That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, United States Code [18 USCS §§ 2510 et seq.], or section 605 of the Communications Act of 1934 [47 USCS § 605], or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if—

(A) it is not reasonable to—

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this title [50 USCS §§ 1801 et seq.]; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(g) Retention of certifications, applications and orders. Certifications made by the Attorney General pursuant to section 102(a) [50 USCS § 1802(a)] and applications made and orders granted under this title [50 USCS §§ 1801 et seq.] shall be retained for a period of at least ten years from the date of the certification or application.

(Oct. 25, 1978, P. L. 95–511, Title I, § 105, 92 Stat. 1790.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Reference in text:

"This Act," referred to in subsec. (d)(2), is Act Oct. 25, 1978, P. L. 95–511, 92 Stat. 1783, popularly known as the Foreign Intelligence Surveillance Act of 1978, which is generally classified to 50 USCS §§ 1801 et seq. For full classification of this Act, consult USCS Tables volumes.

Effective date of section:
Act Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided that this section is generally effective on Oct. 25, 1978. For exception, see note containing Act Oct. 25, 1978, § 301, located at 50 USCS § 1801.

§ 1806. Use of information

(a) Compliance with minimization procedures; privileged communications; lawful purposes. Information acquired from an electronic surveillance conducted pursuant to this title [50 USCS §§ 1801 et seq.] concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this title [50 USCS §§ 1801 et seq.]. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this title [50 USCS §§ 1801 et seq.] shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this title [50 USCS §§ 1801 et seq.] may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Statement for disclosure. No information acquired pursuant to this title [50 USCS §§ 1801 et seq.] shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Notification by United States. Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title [50 USCS §§ 1801 et seq.], the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions. Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title [50 USCS §§ 1801 et seq.], the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Motion to suppress. Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court. Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States of any State before any court or other authority of the United States or any state to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion. If the United States district court pursuant to subsection (f) determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders. Orders granting motions or requests under subsection (g), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information. In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such condents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination. If an emergency employment of electronic

surveillance is authorized under section 105(e) [50 USCS § 1805(e)] and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(Oct. 25, 1978, P. L. 95–511, Title I, § 106, 92 Stat. 1793.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Reference in text:

"This Act," referred to in subsec. (f), is Act Oct. 25, 1978, P. L. 95–511, 92 Stat. 1783, popularly known as the Foreign Intelligence Surveillance Act of 1978, which is generally classified to 50 USCS §§ 1801 et seq. For full classification of this Act, consult USCS Tables volumes.

Effective date of section:

Act Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided that this section is generally effective on Oct. 25, 1978. For exception, see note containing Act Oct. 25, 1978, § 301, located at 50 USCS § 1801.

§ 1807. Report to Administrative Office of the United States Court and to Congress

In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Court and to Congress a report setting forth with respect to the preceding calendar year—

(a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title [50 USCS §§ 1801 et seq.]; and

(b) the total number of such orders and extensions either granted, modified, or denied.

(Oct. 25, 1978, P. L. 95–511, Title I, § 107, 92 Stat. 1795.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Effective date of section:

Act Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided that this section is generally effective on Oct. 25, 1978. For exception, see note containing Act Oct. 25, 1978, § 301, located at 50 USCS § 1801.

§ 1808. Report of Attorney General to congressional committees; limitation on authority or responsibility of information gathering activities of congressional committees; report of congressional committees to Congress

(a) On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all electronic surveillance under this title [50 USCS §§ 1801 et seq.]. Nothing

in this title [50 USCS §§ 1801 et seq.] shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

(b) On or before one year after the effective date of this Act [50 USCS § 1801 note] and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this Act. Said reports shall include but not be limited to an analysis and recommendations concerning whether this Act should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

(Oct. 25, 1978, P. L. 95–511, Title I, § 108, 92 Stat. 1795.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

References in text:

"This Act," referred to in subsec. (b), is Act Oct. 25, 1978, P. L. 95–511, 92 Stat. 1783, popularly known as the Foreign Intelligence Surveillance Act of 1978, which is generally classified to 50 USCS §§ 1801 et seq. For full classification of this Act, consult USCS Tables volumes.

Effective date of section:

Act Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided that this section is generally effective on Oct. 25, 1978. For exception, see note containing Act Oct. 25, 1978, § 301, located at 50 USCS § 1801.

§ 1809. Criminal sanctions

(a) Prohibited activities. A person is guilty of an offense if he intentionally—

(1) engages in electronic surveillance under color of law except as authorized by statute; or

(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

(b) Defense. It is a defense to a prosecution under subsection (a) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(c) Penalties. An offense described in this section is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both.

(d) Federal jurisdiction. There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

(Oct. 25, 1978, P. L. 95–511, Title I, § 109, 92 Stat. 1796.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Effective date of section:

Act Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided that this section is generally effective on Oct. 25, 1978. For exception, see note containing Act Oct. 25, 1978, § 301, located at 50 USCS § 1801.

§ 1810. Civil liability

An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 101(a) or (b)(1)(A) [50 USCS § 1801(a) or (b)(1)(A)], respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 109 [50 USCS § 1809] shall have a cause of action against any person who committed such violation and shall be entitled to recover—
(a) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater;
(b) punitive damages; and
(c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.
(Oct. 25, 1978, P. L. 95–511, Title I, § 110, 92 Stat. 1796.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Effective date of section:
Act Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided that this section is generally effective on Oct. 25, 1978. For exception, see note containing Act Oct. 25, 1978, § 301, located at 50 USCS § 1801.

§ 1811. Authorization during time of war

Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title [50 USCS §§ 1801 et seq.] to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.
(Oct. 25, 1978, P. L. 95–511, Title I, § 111, 92 Stat. 1796.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Effective date of section:
Act Oct. 25, 1978, P. L. 95–511, Title III, § 301, 92 Stat. 1798, provided that this section is generally effective on Oct. 25, 1978. For exception, see note containing Act Oct. 25, 1978, § 301, located at 50 USCS § 1801.

INDEX

An index to material contained in this title will be found at the end of 50 USCS Appendix; see subsequent volume.

APPENDIX C

THE INTELLIGENCE OVERSIGHT ACT OF 1980

Editor's note: The first important statute since 1947 to improve congressional supervision of America's secret services was the Hughes-Ryan Amendment of 1974 (see Appendix A of Volume 3). That law, however, dealt only with covert action. By 1980, Congress had decided to address all intelligence activities, including sensitive collection operations and counterintelligence. Initially, lawmakers had considered passing an omnibus act over 200 pages long, but backed away from such a comprehensive piece of legislation when the intelligence agencies strenuously objected and lobbied effectively to dismantle the "grand charter." In its place came the much abbreviated 1980 act. Though short, it nonetheless had teeth—particularly displayed in its provision that required advance notification of all important intelligence activities, going far beyond the "in a timely manner" reporting requirement embedded in the Hughes-Ryan Act.

(b)(I) The National Security Act of 1947 (50 U.S.C. 401 et seq.) is amended by adding at the end thereof the following new title:

"TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

"CONGRESSIONAL OVERSIGHT

"SEC. 501. (a) To the extent consistent with all applicable authorities and duties, including those conferred by the Constitution upon the executive and legislative branches of the Government, and to the extent consistent with due regard for the protection from unauthorized disclosure of classified information and information relating to intelligence sources and methods, the Director of Central Intelligence and the heads of all departments, agencies, and other entities of the United States involved in intelligence activities shall—

"(I) keep the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives (hereinafter in this section referred to as the 'intelligence committees') fully and currently informed of all intelligence activities which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States, including any significant anticipated intelligence activity, except that (A) the foregoing provision shall not require approval of the intelligence committees as a condition precedent to the initiation of any such anticipated intelligence activity, and (B) if the President determines it is essential to limit prior notice to meet extraordinary circumstances affecting vital interests of the United States, such notice shall be limited to the chairman and ranking minority members of the intelligence committees, the Speaker and minority leader of the House of Representatives, and the majority and minority leaders of the Senate;

"(2) furnish any information or material concerning intelligence activities which is in the possession, custody, or control of any department, agency, or entity of the United States and which is requested by either of the intelligence committees in order to carry out its authorized responsibilities; and

"(3) report in a timely fashion to the intelligence committees any illegal intelligence activity or significant intelligence failure and any corrective action that has been taken or is planned to be taken in connection with such illegal activity or failure.

(b) The President shall fully inform the intelligence committees in a timely fashion of intelligence operations in foreign countries, other than activities intended solely for obtaining necessary intelligence, for which prior notice was not given under subsection (a) and shall provide a statement of the reasons for not giving prior notice.

"(c) The President and the intelligence committees shall each establish such procedures as may be necessary to carry out the provisions of subsections (a) and (b).

"(d) The House of Representatives and the Senate, in consultation with the Director of Central Intelligence, shall each establish, by rule or resolution of such House, procedures to protect from unauthorized disclosure all classified information and all information relating to intelligence sources and methods furnished to the intelligence committees or to Members of the Congress under this section. In accordance with such procedures, each of the intelligence communities shall promptly call to the attention of its respective House, or to any appropriate committee or committees of its respective House, any matter relating to intelligence activities requiring the attention of such House or such committee or committees.

"(e) Nothing in this Act shall be construed as authority to withhold information from the intelligence committees on the grounds that providing the information to the intelligence committees would constitute the unauthorized disclosure of classified information or information relating to intelligence sources and methods."

(2) The table of contents at the beginning of such Act is amended by adding at the end thereof the following:

"TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

"Sec. 501. Congressional oversight."

APPENDIX D

THE INTELLIGENCE OVERSIGHT ACT OF 1991

Editor's note: In the aftermath of the Iran-*contra* affair, lawmakers tried again to improve the statutory framework for intelligence accountability. The result was the Intelligence Oversight Act of 1991, reprinted here, which defined covert action more sharply; required the President to sign all "findings" (oral approvals, as used by President Ronald Reagan, would no longer suffice); and clarified the reporting requirements for covert actions, with a slight congressional concession in favor of presidential delay in reporting during times of acute national emergencies. In such cases, the president could postpone reporting for a couple of days, rather than honoring the "prior notice" provision of the 1980 Intelligence Oversight Act.

TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES[1]

GENERAL CONGRESSIONAL OVERSIGHT PROVISIONS

SEC. 501. [50 U.S.C. 413] (a) (1) The President shall ensure that the intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this title.

(2) As used in this title, the term "intelligence committees" means the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

---

[1] This title is also set out *post* at page 409 along with other materials relating to congressional oversight of intelligence activities.

(3) Nothing in this title shall be construed as requiring the approval of the intelligence committees as a condition precedent to the initiation of any significant anticipated intelligence activity.

(b) The President shall ensure that any illegal intelligence activity is reported promptly to the intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity.

(c) The President and the intelligence committees shall each establish such procedures as may be necessary to carry out the provisions of this title.

(d) The House of Representatives and the Senate shall each establish, by rule or resolution of such House, procedures to protect from unauthorized disclosure all classified information, and all information relating to intelligence sources and methods, that is furnished to the intelligence committees or to Members of Congress under this title. Such procedures shall be established in consultation with the Director of Central Intelligence. In accordance with such procedures, each of the intelligence committees shall promptly call to the attention of its respective House, or to any appropriate committee or committees of its respective House, any matter relating to intelligence activities requiring the attention of such House or such committee or committees.

(e) Nothing in this Act shall be construed as authority to withhold information from the intelligence committees on the grounds that providing the information to the intelligence committees would constitute the unauthorized disclosure of classified information or information relating to intelligence sources and methods.

(f) As used in this section, the term "intelligence activities" includes covert actions as defined in section 503(e).

REPORTING OF INTELLIGENCE ACTIVITIES OTHER THAN COVERT ACTIONS

SEC 502. [50 U.S.C. 413a] To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of Central Intelligence and the heads of all departments, agencies, and other entities of the United States Government involved in intelligence activities shall—

(1) keep the intelligence committees fully, and currently informed of all intelligence activities, other than a covert action (as defined in section 503(e)), which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including any significant anticipated intelligence activity and any significant intelligence failure; and

(2) furnish the intelligence committees any information or material concerning intelligence activities, other than covert actions, which is within their custody or control, and which is requested by either of the intelligence committees in order to carry out its authorized responsibilities.

PRESIDENTIAL APPROVAL AND REPORTING OF COVERT ACTIONS

SEC 503. [50 U.S.C. 413b] (a) The President may not authorize the conduct of a covert action by departments, agencies, or entities of the United States Government unless the

President determines such an action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States, which determination shall be set forth in a finding that shall meet each of the following conditions:

(1) Each finding shall be in writing, unless immediate action by the United States is required and time does not permit the preparation of a written finding, in which case a written record of the President's decision shall be contemporaneously made and shall be reduced to a written finding as soon as possible but in no event more than 48 hours after the decision is made.

(2) Except as permitted by paragraph (1), a finding may not authorize or sanction a covert action, or any aspect of any such action, which already has occurred.

(3) Each finding shall specify each department, agency, or entity of the United States Government authorized to fund or otherwise participate in any significant way in such action. Any employee, contractor, or contract agent of a department, agency, or entity of the United States Government other than the Central Intelligence Agency directed to participate in any way in a covert action shall be subject either to the policies and regulations of the Central Intelligence Agency, or to written policies or regulations adopted by such department, agency, or entity, to govern such participation.

(4) Each finding shall specify whether it is contemplated that any third party which is not an element of, or a contractor or contract agent of, the United States Government, or is not otherwise subject to United States Government policies and regulations, will be used to fund or otherwise participate in any significant way in the covert action concerned, or be used to undertake the covert action concerned on behalf of the United States.

(5) A finding may not authorize any action that would violate the Constitution or any statute of the United States.

(b) To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of Central Intelligence and the heads of all departments, agencies, and entities of the United States Government involved in a covert action—

(1) shall keep the intelligence committees fully and currently informed of all covert actions which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including significant failures; and

(2) shall furnish to the intelligence committees any information or material concerning covert actions which is in the possession, custody, or control of any department, agency, or entity of the United States Government and which is requested by either of the intelligence committees in order to carry out its authorized responsibilities.

(c)(1) The President shall ensure that any finding approved pursuant to subsection (a) shall be reported to the intelligence committees as soon as possible after such approval and before the initiation of the covert action authorized by the finding, except as otherwise provided in paragraph (2) and paragrap (3).

(2) If the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States, the finding may

be reported to the chairmen and ranking minority members of the intelligence committees, the Speaker and minority leader of the House of Representatives, the majority and minority leaders of the Senate, and such other member or members of the congressional leadership as may be included by the President.

(3) Whenever a finding is not reported pursuant to paragraph (1) or (2) of this section, the President shall fully inform the intelligence committees in a timely fashion and shall provide a statement of the reasons for not giving prior notice.

(4) In a case under paragraph (1), (2), or (3), a copy of the finding, signed by the President, shall be provided to the chairman of each intelligence committee. When access to a finding is limited to the Members of Congress specified in paragraph (2), a statement of the reasons for limiting such access shall also be provided.

(d) The President shall ensure that the intelligence committees, or, if applicable, the Members of Congress specified in subsection (c)(2), are notified of any significant change in a previously approved covert action, or any significant undertaking pursuant to a previously approved finding, in the same manner as findings are reported pursuant to subsection (c).

(e) As used in this title, the term "covert action" means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include—

(1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

(2) traditional diplomatic or military activities or routine support to such activities;

(3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(f) No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

FUNDING OF INTELLIGENCE ACTIVITIES

SEC 504. **[**50 U.S.C. 414**]** (a) Appropriated funds available to an intelligence agency may be obligated or expended for an intelligence or intelligence-related activity only if—

(1) those funds were specifically authorized by the Congress for use for such activities; or

(2) in the case of funds from the Reserve for Contingencies of the Central Intelligence Agency and consistent with the provisions of section 503 of this Act concerning any significant anticipated intelligence activity, the Director of Central Intelligence has notified the appropriate congressional committees of the intent to make such funds available for such activity; or

(3) in the case of funds specifically authorized by the Congress for a different activity—

(A) the activity to be funded is a higher priority intelligence or intelligence-related activity;

(B) the need for funds for such activity is based on unforseen requirements; and

(C) the Director of Central Intelligence, the Secretary of Defense, or the Attorney General, as appropriate, has notified the appropriate congressional committees of the intent to make such funds available for such activity;

(4) nothing in this subsection prohibits obligation or expenditure of funds available to an intelligence agency in accordance with sections 1535 and 1536 of title 31, United States Code.

(b) Funds available to an intelligence agency may not be made available for any intelligence or intelligence-related activity for which funds were denied by the Congress.

(c) No funds appropriated for, or otherwise available to, any department, agency, or entity of the United States Government may be expended, or may be directed to be expended, for any covert action, as defined in section 503(e), unless and until a Presidential finding required by subsection (a) of section 503 has been signed or otherwise issued in accordance with that subsection.

(d)(1) Except as otherwise specifically provided by law, funds available to an intelligence agency that are not appropriated funds may be obligated or expended for an intelligence or intelligence-related activity only if those funds are used for activities reported to the appropriate congressional committees pursuant to procedures which identify—

(A) the types of activities for which nonappropriated funds may be expended; and

(B) the circumstances under which an activity must be reported as a significant anticipated intelligence activity before such funds can be expended.

(2) Procedures for purposes of paragraph (1) shall be jointly agreed upon by the intelligence committees and, as appropriate, the Director of Central Intelligence or the Secretary of Defense.

(e) As used in this section—

(1) the term "intelligence agency" means any department, agency, or other entity of the United States involved in intelligence or intelligence-related activities;

(2) the term "appropriate congressional committees" means the Permanent Select Committee on Intelligence and the Committee on Appropriations of the House of Representatives and the Select Committee on Intelligence and the Committee on Appropriations of the Senate; and

(3) the term "specifically authorized by the Congress" means that—

(A) the activity and the amount of funds proposed to be used for that activity were identified in a formal budget request to the Congress, but funds shall be deemed to be specifically authorized for that activity only to the extent that the Congress both authorized the funds to be appropriated for that activity and appropriated the funds for that activity; or

(B) although the funds were not formally requested, the Congress both specifically authorized the appropriation of the funds for the activity and appropriated the funds for the activity.

NOTICE TO CONGRESS OF CERTAIN TRANSFERS OF DEFENSE ARTICLES AND DEFENSE SERVICES

SEC 505. [50 U.S.C. 415] (a)(1) The transfer of a defense article or defense service, or the anticipated transfer in any fiscal year of any aggregation of defense articles or defense services, exceeding $1,000,000 in value by an intelligence agency to a recipient outside that agency shall be considered a significant anticipated intelligence activity for the purpose of this title.

(2) Paragraph (1) does not apply if—

(A) the transfer is being made to a department, agency, or other entity of the United States (so long as there will not be a subsequent retransfer of the defense articles or defense services outside the United States Government in conjunction with an intelligence or intelligence-related activity); or

(B) the transfer—

(i) is being made pursuant to authorities contained in part II of the Foreign Assistance Act of 1961, the Arms Export Control Act, title 10 of the United States Code (including a law enacted pursuant to section 7307(b)(1) of that title), or the Federal Property and Administrative Services Act of 1949, and

(ii) is not being made in conjunction with an intelligence or intelligence-related activity.

(3) An intelligence agency may not transfer any defense articles or defense services outside the agency in conjunction with any intelligence or intelligence-related activity for which funds were denied by the Congress.

(b) As used in this section—

(1) the term "intelligence agency" means any department, agency, or other entity of the United States involved in intelligence or intelligence-related activities;

(2) the terms "defense articles" and "defense services" mean the items on the United States Munitions List pursuant to section 38 of the Arms Export Control Act (22 CFR part 121);

(3) the term "transfer" means—

(A) in the case of defense articles, the transfer of possession of those articles; and

(B) in the case of defense services, the provision of those services; and

(4) the term "value" means—

(A) in the case of defense articles, the greater of—

(i) the original acquisition cost to the United States Government, plus the cost of improvements or other modifications made by or on behalf of the Government; or

(ii) the replacement cost; and

(B) in the case of defense services, the full cost to the Government of providing the services.

APPENDIX E

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE CONCLUSIONS ON INTELLIGENCE OVERSIGHT, 1996

Editor's note: In 1995–96, both the White House and the U.S. House conducted inquiries into the state of intelligence, prompted by the revelations about the Aldrich Ames counterintelligence failure as well as a sense that the end of the Cold War meant dramatic changes would be necessary in America's global intelligence activities. The Aspin-Brown Commission led the White House inquiry. The House Permanent Select Committee on Intelligence named its investigation "IC21," standing for the Intelligence Community in the 21st century. This appendix offers the summary conclusions of the House Committee on how to improve intelligence oversight.

CONGRESSIONAL OVERSIGHT

The modern system of congressional oversight of intelligence—select committees in the House and in the Senate specifically devoted to intelligence—is almost twenty years old. Reviewing the strengths and weaknesses of this system, as well as the contribution that congressional oversight can and should make to intelligence is appropriate as part of the larger *IC21* study.

Issues regarding congressional oversight fall into two large categories: the general nature of how Congress carries out oversight and specific issues of organization and process related to intelligence oversight. Although this report touches on some generic issues of intelligence oversight, its findings and recommendations are restricted to the way in which the House of Representatives handles this function.

Source: "IC21: Intelligence Community in the 21st Century," *Staff Study*, Permanent Select Committee on Intelligence, House of Representatives, 104th Cong. 2d Sess. (1996), pp. 313–330.

BACKGROUND: EVOLUTION OF CONGRESSIONAL OVERSIGHT OF INTELLIGENCE

It is important to recall how the current intelligence oversight system came into being. The two select committees were the direct result of the congressional (and executive) investigations into U.S. intelligence activities in 1975–76. Both Houses came to the conclusion that the past oversight system had been inadequate in terms of both the vigor with which it was carried out[1] and the very limited number of Members who were privy to intelligence-related information. That older system reflected the gentleman's agreement nature of oversight that evolved during the Cold War. It accepted the necessity of intelligence—and especially of intelligence activities (i.e., covert action), but treated them in an extraordinary manner because of their highly classified and extremely sensitive nature.

The House Permanent Select Committee on Intelligence (HPSCI) was established on July 14, 1977 by H. Res. 658 of the 95th Congress and is governed by Rule XLVIII of the Rules of the House. The current system attempted to correct the main flaws in the older system in two major ways. First, the House decided that a committee with specific oversight over intelligence (albeit with different jurisdictions in the House and Senate) was necessary to ensure more vigorous and regular oversight. Second, in order to broaden the oversight base, each committee has "cross-over" Members from other committees that have an interest in intelligence or intelligence related issues: Appropriations; International Relations; Judiciary; and National Security.

However, and this is perhaps ironic, the House continued to treat intelligence as something extraordinary, rather than as an accepted function of government similar to any others that are subject to oversight. This is reflected in two aspects of HPSCI. First, it is a select committee rather than a standing committee. Second, and derived from the first, are the rules limiting the length of consecutive service on the Committee. These tenure rules arose from the perception that the past intelligence overseers had grown "too cozy" with the intelligence agencies, thus becoming less vigorous in their oversight. Rotating the membership on a regular basis, it was believed, would avoid this type of overly close and potentially less critical relationship in the future.

THE NATURE OF OVERSIGHT: ADVERSARY VS. ADVOCATE

Each committee charged with congressional oversight has a dual responsibility. The most obvious is to oversee the various agencies under its mandate, approve their budgets, investigate known or suspected problems, and report back to the House on these matters. Recognizing the impossibility of each Member being conversant with (or intensely

[1] The most-oft cited example of the problem was the quote from Senator Leverett Saltonstall, a member of the Armed Services Committee, which was responsible for intelligence oversight. When asked by Senator Mike Mansfield why there had only been two committee meetings with the CIA in the past year, Senator Saltonstall replied: "... it is not a question of reluctance on the part of the CIA officials to speak to us. Instead, it is a question of our reluctance, if you will, to seek information and knowledge on subjects which I personally, as a Member of Congress and as a citizen, would rather not have, unless I believed it to be my responsibility to have it because it might involve the lives of American citizens." *Congressional Record,* April 9, 1956, p. 5924.

interested in) all issues, the committee system delegates responsibility to the committees and accepts their leadership in specific areas. Given the checks and balances nature of the congressional-executive relationship, each committee has, at some level, an adversarial role with its Executive Branch opposites. The relationship need not be overtly or continuously hostile, but there is inevitably a certain amount of friction involved.

The responsibility for being the House's resident experts on given programs and agencies also gives rise to a second role for each oversight committee, that of advocacy for those agencies and programs. It is only natural that those Members most interested in and most conversant with agencies and programs will also, on occasion, be their advocates. Increasingly constrained debates over budget shares, disinterest or outright hostility from other Members about agencies or programs for a wide variety of reasons, all put oversight committees in this advocacy role as well.

Oversight, if carried out properly, should be a combination of these two roles. An excessive concentration on either will damage the ability of the committee to handle its issues effectively and can undermine the credibility of that committee among its colleagues.

However, it is not clear that this norm of oversight behavior is widely accepted as proper for HPSCI. The fact that intelligence continues to be handled as an extraordinary issue in terms of oversight—by virtue of a select committee and tenure limits—suggests that it was at least expected at its origin that HPSCI would largely eschew advocacy role and that this expected emphasis on adversary rather than advocate has been tacitly accepted over the last twenty years.

There remains a lingering uneasiness about intelligence and its role in the U.S. government that will never be completely resolved. At some level, the concept of secret agencies with classified budgets runs counter to some deeply felt view of what and how the U.S. government should behave. However, this less than full acceptance may actually be heightened rather than pacified by the current oversight system, which treats intelligence in a manner different from other government activities.

Interestingly, several witnesses who appeared before HPSCI during *IC21* hearings made the same point: intelligence, unlike virtually all other functions of government, has no natural advocates in the public at large. Its direct effect on the lives of most citizens is largely unfelt or unseen; its industrial base is too rarefied to build a large constituency in many areas; it is largely an "inside the Beltway" phenomenon in terms of location, logistics, budget and concern. The only places where intelligence can hope to find some base level of support are from its Executive Branch masters and its congressional overseers.[2]

By having HPSCI as a select committee, Congress is, in effect, *elevating* intelligence. It is seen as an extraordinary issue requiring congressional organizational responses that depart from the norm. At some levels, this view of intelligence is accurate, but this also adds to the mystique that too often surrounds intelligence and often engenders wariness about it on the part of some Members. By making HPSCI a standing committee, intelligence would be treated like other "normal" functions of government. Making intelligence a less extraordinary issue might actually have positive effects, in that by being seen as less unique the very *raison* of the IC might not be questioned as much.

[2] Testimony of Richard Helms and James Schlesinger before House Permanent Select Committee on Intelligence on May 22, 1995.

THE PROPRIETY OF CONGRESSIONAL OVERSIGHT OF INTELLIGENCE

Not surprisingly, we believe that the modern oversight system for intelligence residing in committees specifically devoted to that task has worked well. The House and Senate committees have achieved the two main goals of their founders in the 94th and 95th Congresses, creating a system that is more vigorous and more rigorous and is more broadly based than the previous system. All oversight is imperfect and is always limited by the degree to which the Executive Branch will be forthcoming with information. Given the highly classified and often compartmented nature of intelligence information, this may be a more exacting problem for the intelligence committees. Nonetheless, we continue to believe that the current system has largely been effective.

We also do not see that any alternative to having a distinct committee oversee intelligence is preferable. Each oversight committee finds itself with a full agenda. Returning oversight to the House National Security Committee (HNSC) would act to the detriment of both those Members charged with intelligence oversight and the intelligence agencies themselves.

We also understand that there will always be some in the intelligence agencies who will question, resent and perhaps resist the idea of Congress having extensive oversight powers. This view is not unique to intelligence. It is unlikely that there is any Executive agency or department that does not harbor similar sentiments at some time. Still, this feeling may run deeper in the Intelligence Community. Sharing information with "outsiders," even if they are elected officials, runs counter to the ethos of intelligence as some understand it. We are also aware of repeated complaints by intelligence agency heads about the amount of time they must spend either before Congress or responding to Congress. Again, this sentiment is not unique, and we are also not convinced that the burden is any more onerous for intelligence agencies than for any others.

Effective oversight and an informed Congress are now considered among the expected norms of our system of government. We believe that oversight, if carried out seriously and with a modicum of support from intelligence agencies, not only helps ensure greater Executive branch effectiveness and propriety, but can also be a substantial force in rebuilding a sorely needed consensus to support intelligence agencies, prorams and activities.

A JOINT COMMITTEE

The issue of a joint congressional committee to oversee intelligence has been proposed in virtually every Congress since 1976. The main arguments in favor of a joint committee are:

- It would restrict the number of Members and staff (currently 33 Members and 50 staff in the House and Senate Committees) with access to highly classified information, thus limiting the possibility of unauthorized disclosures.
- It would underscore the seriousness with which Congress views intelligence, by handling it in this manner, similar to how atomic energy (i.e., nuclear weapons development and proliferation) issues were overseen from 1946–1977 by the Joint Committee on Atomic Energy.

The main arguments against a joint committee are:

- Concern over restricting the number of Members and staff with access to intelligence information implies that Congress cannot be trusted with such information. Although the record of Congress with regard to safeguarding such information is not perfect, it remains far better than Executive Branch agencies. Congress must be vigilant in this regard, but this does not argue that current number need to be further restricted.
- By creating a joint committee, Congress would further heighten the view that intelligence is an extraordinary, rather than an accepted, function of government. No other executive branch agencies or functions are overseen by a joint committee, thus raising the issue of why intelligence needs to be overseen in this manner.
- The oversight scope of the two current intelligence committees are not identical. Intelligence programs are currently divided into three broad groups: *NFIP: the National Foreign Intelligence Program,* which includes the Director of Central Intelligence; CIA; and the national foreign intelligence or counterintelligence programs of the Defense Department, DIA, NSA, the Central Imagery Office, NRO, Army, Navy and the Air Force, the Departments of State, Treasury and Energy, the FBI and DEA; *JMIP: the Joint Military Intelligence Program,* covering intelligence for defense-wide or theater-level consumers; and *TIARA: Tactical Intelligence and Related Activities,* covering service unique and tactical intelligence needs. HPSCI oversees all of these intelligence programs, sharing oversight of TIARA with the HNSC. The Senate Select Committee on Intelligence (SSCI) oversees only the NFIP. To create a joint committee, one House or the other would have to make substantial changes in the scope of oversight accorded to this new committee.
- It is highly questionable that the establishment of a joint committee would significantly reduce the number of Members and staffers that currently have access to classified information. No committee system will make Congress "leak proof." Even with a joint committee, there still would be a substantial number of Members and staff with access to intelligence information across several House Committees (Appropriations, National Security, Judiciary, International Relations), as well as their Senate counterparts.
- The joint committee structure is not suitable to an authorizing committee as it would complicate Congressional efforts to conduct our necessary oversight activities. By shrinking the number of Members familiar with the Intelligence Community, an inevitable result will be a diminution in Members' knowledge of the complexities of intelligence oversight. Additionally, the current system of two separate intelligence committees provides a more effective system of Constitutional checks and balances on Executive Branch activities.

Finding: There is no compelling reason to convert the current system to a joint committee. As noted, Congress's record regarding safeguarding highly classified information is not perfect, but does not warrant this step. Creating a joint committee would also require either the House or the Senate to alter its current arrangements for intelligence oversight, which has not had significant support in the past. Finally, and most importantly, creating a joint committee for intelligence would continue to heighten the view that intelligence is something other than an accepted function of government, which tends to increase rather than complement oversight issues and problems.

SELECT COMMITTEE/APPOINTMENT AND TENURE LIMITS

The reasons for these two aspects of the current oversight structure are described above. Although specific provisions for a standing intelligence committee could be established, changing HPSCI into a standing committee would *most likely* (but not necessarily) affect the process of assignment and lengths of service.

The main arguments in favor of the current select committee arrangement relating to assignment procedures are: [still-classified section missing text]

CONCLUSION: FINDINGS AND RECOMMENDATIONS

FINDINGS

- The current intelligence oversight system arose from a view that intelligence had to be handled in a manner that was extraordinary when compared to other functions of government. Although that view may have been warranted in the aftermath of the investigations in 1975–76, it is not warranted any longer. Indeed, by continuing to view intelligence in this manner, oversight and the work of the Intelligence Community are likely made more difficult.
- Advocacy for overseen agencies is legitimate and to some extent necessary. This has not been an accepted stance for the intelligence committees. We agree with the view of former DCIs that intelligence is such a restricted issue that Congress must be more active in building the necessary political consensus.
- The current oversight system has been largely effective, and clearly has responded to those problems that prompted the creation of the current committees.
- There is no compelling reason to convert the current system to a joint committee. As noted, Congress's record regarding safeguarding highly classified information is not perfect, but does not warrant this step. Creating a joint committee would also require either the House or the Senate to alter its current arrangements for intelligence oversight, which has not had significant support in the past. Finally, and most importantly, creating a joint committee for intelligence would continue to heighten the view that intelligence is something other than an accepted function of government, which tends to increase rather than complement oversight issues and problems.
- Although the reasons for which the current committee was made a select committee with tenure limits may have been valid in 1977, these may no longer be compelling or valid. There are equally compelling arguments in terms of the general effect of these arrangements on oversight to warrant reconsidering them.
- Unauthorized disclosures of classified information by Members or staff should trigger thorough investigations relying on strict enforcement of the applicable Federal statutes and House rules. Any individual who is conclusively determined to be the source of such unauthorized disclosures should be subject to the full range of penalties prescribed by the law. The rules promulgated by the Committee on Standards of Official Conduct on July 12, 1995 should be strictly and consistently enforced by HPSCI.
- The current oversight structure puts intelligence—as both a government function and as an issue—at a distinct disadvantage. Unlike other national security functions, congressional oversight of intelligence is neither unified nor clearly delineated. The

prime effect of this arrangement is seen in the degree to which intelligence programs are subjected to budget cuts largely because of *how* they are dealt with (i.e., as part of the defense authorization and appropriations process), rather than on their own merits.

RECOMMENDATIONS

- It is important that the House act to "normalize" the way in which it oversees intelligence. By continuing to handle intelligence as an extraordinary function, the current oversight system predicates an approach that may be overly adversarial and may actually make effective oversight more difficult.
- The House should give serious consideration to converting HPSCI to a standing committee, with no limits on terms of service for Members. This would help "normalize" intelligence and greatly improve expertise and continuity on the Committee.
- The House should consider allowing HPSCI to have exclusive jurisdiction over all aspects of intelligence that are part of the larger intelligence architecture, while the HNSC has exclusive jurisdiction over those aspects of intelligence solely related to military intelligence needs but that are not part of this larger architecture. Second, the House should consider creating a separate appropriations subcommittee exclusively for intelligence.
- The House should seek to better protect Intelligence Community equities by erecting legislative "firewalls" between HPSCI and HNSC during the authorization phase; similarly, efforts should be made to establish mechanisms for better legislative consultation and coordination with the House Appropriations Committee during the appropriations phase.
- Establish a semi-annual strategic intelligence review meeting between the new Committee on Foreign Intelligence (CFI) and the intelligence committees.

APPENDIX F

9/11 COMMISSION CONCLUSIONS ON INTELLIGENCE OVERSIGHT, 2004

Editor's note: Eight years after the IC21 Report, the 9/11 Commission also took a look—albeit brief—at the state of intelligence accountability. Its conclusion was blunt: the whole system of oversight had become "dysfunctional." This appendix provides the language of the Commission on the subject of weaknesses in the legislative supervision of America's intelligence agencies.

13.4 UNITY OF EFFORT IN THE CONGRESS

Strengthen Congressional Oversight of Intelligence and Homeland Security

Of all our recommendations, strengthening congressional oversight may be among the most difficult and important. So long as oversight is governed by current congressional rules and resolutions, we believe the American people will not get the security they want and need. The United States needs a strong, stable, and capable congressional committee structure to give America's national intelligence agencies oversight, support, and leadership.

Few things are more difficult to change in Washington than congressional committee jurisdiction and prerogatives. To a member, these assignments are almost as important as the map of his or her congressional district. The American people may have to insist that these changes occur, or they may well not happen. Having interviewed numerous members of Congress from both parties, as well as congressional staff members, we found that dissatisfaction with congressional oversight remains widespread.

The future challenges of America's intelligence agencies are daunting. They include the need to develop leading-edge technologies that give our policy-makers and warfighters

---

Source: *The 9/11 Report*, The National Commission on Terrorist Attacks Upon the United States (the Kean Commission), Washington, D.C., 2004, pp. 419–423.

a decisive edge in any conflict where the interests of the United States are vital. Not only does good intelligence win wars, but the best intelligence enables us to prevent them from happening altogether.

Under the terms of existing rules and resolutions the House and Senate intelligence committees lack the power, influence, and sustained capability to meet this challenge. While few members of Congress have the broad knowledge of intelligence activities or the know-how about the technologies employed, all members need to feel assured that good oversight is happening. When their unfamiliarity with the subject is combined with the need to preserve security, a mandate emerges for substantial change.

Tinkering with the existing structure is not sufficient. Either Congress should create a joint committee for intelligence, using the Joint Atomic Energy Committee as its model, or it should create House and Senate committees with combined authorizing and appropriations powers.

Whichever of these two forms are chosen, the goal should be a structure—codified by resolution with powers expressly granted and carefully limited—allowing a relatively small group of members of Congress, given time and reason to master the subject and the agencies, to conduct oversight of the intelligence establishment and be clearly accountable for their work. The staff of this committee should be nonpartisan and work for the entire committee and not for individual members.

The other reforms we have suggested—for a National Counterterrorism Center and a National Intelligence Director—will not work if congressional oversight does not change too. Unity of effort in executive management can be lost if it is fractured by divided congressional oversight.

Recommendation: Congressional oversight for intelligence—and counterterrorism—is now dysfunctional. Congress should address this problem. We have considered various alternatives: A joint committee on the old model of the joint Committee on Atomic Energy is one. A single committee in each house of Congress, combining authorizing and appropriating authorities, is another.

- The new committee or committees should conduct continuing studies of the activities of the intelligence agencies and report problems relating to the development and use of intelligence to all members of the House and Senate.
- We have already recommended that the total level of funding for intelligence be made public, and that the national intelligence program be appropriated to the National Intelligence Director, not to the secretary of defense.[19]
- We also recommend that the intelligence committee should have a subcommittee specifically dedicated to oversight, freed from the consuming responsibility of working on the budget.
- The resolution creating the new intelligence committee structure should grant subpoena authority to the committee or committees. The majority party's representation on this committee should never exceed the minority's representation by more than one.
- Four of the members appointed to this committee or committees should be a member who also serves on each of the following additional committees: Armed Services, Judiciary, Foreign Affairs, and the Defense Appropriations subcommittee. In this way the other major congressional interests can be brought together in the new committee's work.

- Members should serve indefinitely on the intelligence committees, without set terms, thereby letting them accumulate expertise.
- The committees should be smaller—perhaps seven or nine members in each house—so that each member feels a greater sense of responsibility, and accountability, for the quality of the committee's work.

The leaders of the Department of Homeland Security now appear before 88 committees and subcommittees of Congress. One expert witness (not a member of the administration) told us that this is perhaps the single largest obstacle impeding the department's successful development. The one attempt to consolidate such committee authority, the House Select Committee on Homeland Security, may be eliminated. The Senate does not have even this.

Congress needs to establish for the Department of Homeland Security the kind of clear authority and responsibility that exist to enable the Justice Department to deal with crime and the Defense Department to deal with threats to national security. Through not more than one authorizing committee and one appropriating subcommittee in each house, Congress should be able to ask the secretary of homeland security whether he or she has the resources to provide reasonable security against major terrorist acts within the United States and to hold the secretary accountable for the department's performance.

Recommendation: Congress should create a single, principal point of oversight and review for homeland security. Congressional leaders are best able to judge what committee should have jurisdiction over this department and its duties. But we believe that Congress does have the obligation to choose one in the House and one in the Senate, and that this committee should be a permanent standing committee with a nonpartisan staff.

Improve the Transitions between Administrations

In chapter 6, we described the transition of 2000–2001. Beyond the policy issues we described, the new administration did not have its deputy cabinet officers in place until the spring of 2001, and the critical subcabinet officials were not confirmed until the summer—if then. In other words, the new administration—like others before it—did not have its team on the job until at least six months after it took office.

Recommendation: Since a catastrophic attack could occur with little or no notice, we should minimize as much as possible the disruption of national security policymaking during the change of administrations by accelerating the process for national security appointments. We think the process could be improved significantly so transitions can work more effectively and allow new officials to assume their new responsibilities as quickly as possible.

- Before the election, candidates should submit the names of selected members of their prospective transition teams to the FBI so that, if necessary, those team members can obtain security clearances immediately after the election is over.
- A president-elect should submit lists of possible candidates for national security positions to begin obtaining security clearances immediately after the election, so that their background investigations can be complete before January 20.
- A single federal agency should be responsible for providing and maintaining security clearances, ensuring uniform standards—including uniform security

questionnaires and financial report requirements, and maintaining a single database. This agency can also be responsible for administering polygraph tests on behalf of organizations that require them.

- A president-elect should submit the nominations of the entire new national security team, through the level of under secretary of cabinet departments, not later than January 20. The Senate, in return, should adopt special rules requiring hearings and votes to confirm or reject national security nominees within 30 days of their submission. The Senate should not require confirmation of such executive appointees below Executive Level 3.
- The outgoing administration should provide the president-elect, as soon as possible after election day, with a classified, compartmented list that catalogues specific, operational threats to national security; major military or covert operations; and pending decisions on the possible use of force. Such a document could provide both notice and a checklist, inviting a president-elect to inquire and learn more.

NOTE

19. This change should eliminate the need in the Senate for the current procedure of sequential referral of the annual authorization bill for the national foreign intelligence program. In that process, the Senate Armed Services Committee reviews the bill passed by the Senate Select Committee on Intelligence before the bill is brought before the full Senate for consideration.

APPENDIX G

DOCUMENTS ON INTELLIGENCE FUNDING

Editor's note: In 1995–96, the Aspin-Brown Commission Report examined a wide range of intelligence issues in the United States. This appendix contains the Commission's main findings about intelligence funding—a key aspect of maintaining accountability for the secret agencies.

THE NEED FOR AN EFFECTIVE BUDGET STRUCTURE AND PROCESS

The annual budgets for U.S. intelligence organizations constitute one of the principal vehicles for managing intelligence activities. They reflect decisions on whether to expand or cut existing activities and whether to initiate new ones, thereby molding future capabilities. How effectively and efficiently the Intelligence Community operates is to a large degree a function of how these budgets are put together and how they are approved and implemented.

The budget process for most departments and agencies is relatively straightforward. A budget is prepared in accordance with the funding level approved by the President and submitted to Congress as part of the President's annual budget. After its review, the Congress appropriates funds for the agency concerned.

Where intelligence—a function, rather than an agency—is concerned, the budget process is more complex. This complexity exists essentially for two reasons. The DCI is

---

Source: *Preparing for the 21st Century: An Appraisal of U.S. Intelligence,* Report of the Commission on the Roles and Capabilities of the United States Intelligence Community (the Aspin-Brown Commission, led first by former Secretary of Defense Les Aspin and then, when he passed away during the inquiry, by former Secretary of Defense Harold Brown), Washington, D.C., March 1, 1996, pp. 71–82, 131–138.

charged by law with developing and approving a budget for "national" foreign intelligence activities that cut across departmental and agency lines. In addition, the budget developed by the DCI for "national" intelligence activities is but one of three resource aggregations that make up the overall intelligence budget. The other two aggregations are funded separately by the Department of Defense.

The implications of this arrangement for the DCI and the intelligence function are explained below.

The National Foreign Intelligence Program Budget

The budget for national intelligence programs is known as the National Foreign Intelligence Program (NFIP) budget. In theory, the NFIP funds all of the foreign intelligence and counterintelligence activities of the Government that respond to "national" needs, as opposed to the needs of a single department or agency. Put another way, it funds the activities of the U.S. Intelligence Community, as defined in law and described in this report.[1]

Intelligence activities compete with other funding priorities of the parent department or agency that manages the intelligence unit(s). The funds appropriated for NFIP activities are made available to the parent department or agency and not to the DCI.[2] Thus, intelligence funds represent a part of the budgets of the several departments and agencies which maintain intelligence elements with national responsibilities. In developing a single "national" foreign intelligence budget, the DCI must first accommodate the funding levels and priorities of the department or agency that "owns" the intelligence element(s) concerned. At the same time, the DCI must devise an overall intelligence program to satisfy national needs.

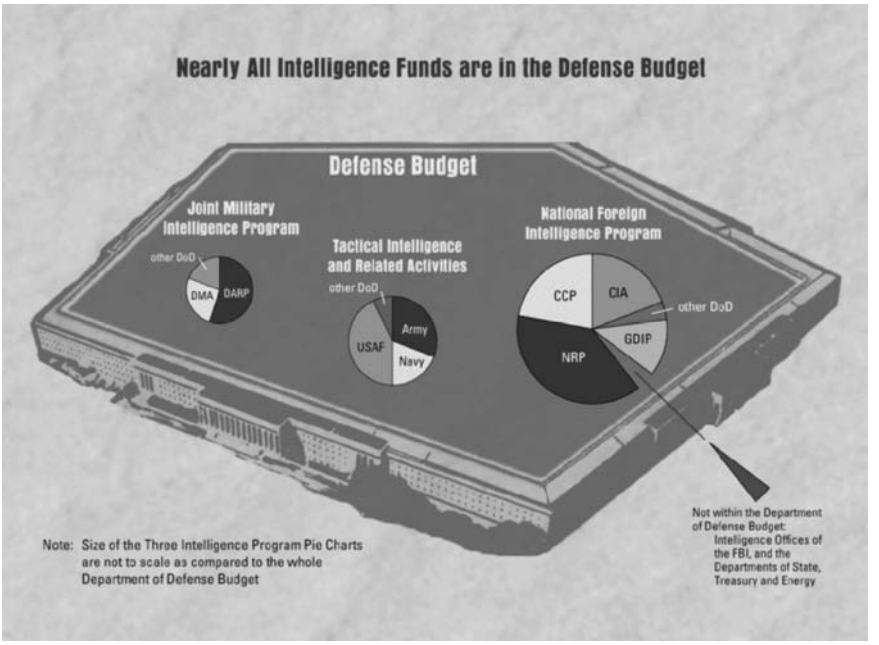
DoD "owns" the preponderance of national intelligence capabilities and its intelligence spending accounts for about three-fourths of the NFIP. When DoD spending is combined with CIA spending (which also is funded in the Defense budget for secrecy reasons), they constitute virtually all of the total budget for national intelligence. For all practical purposes, therefore, the amount determined by the Secretary of Defense, in consultation with the DCI, for "national" intelligence activities within the Defense budget *is* the National Foreign Intelligence Program budget.

From the overall level established for the NFIP, the DCI establishes funding levels for certain component "programs," each of which is administered by a separate "program manager."[3] These program managers perform the detailed work of assembling the budgets for each program which are ultimately reviewed and submitted to the DCI for approval. To succeed in their task, program managers must understand the information requirements

[1] The intelligence organizations of the Departments of the Army, Navy, and Air Force also receive significant funding outside of the NFIP.

[2] Funding for the CIA is appropriated to the Department of Defense, which transfers it to the CIA.

[3] As generally used in this report, "program managers" refers to those individuals who formulate the budget of a particular subcomponent, or program, within the NFIP. For example, the program managers of the four largest NFIP subcomponents are the Director, NRO (for the National Reconnaissance Program); the Director, NSA (for the Consolidated Cryptologic Program); the Executive Director, CIA (for the Central Intelligence Agency Program); and the Director, DIA (for the General Defense Intelligence Program). However, there are other intelligence program managers, such as the Director, Defense Airborne Reconnaissance Office (for the Defense Airborne Reconnaissance Program, a subcomponent of DoD's Joint Military Intelligence Program).



likely to be placed on them and decide how best to satisfy them. For the costly technical disciplines, program managers must try to divine what technological capabilities are likely to be available and needed during the next five to 10 years so that funding can be included in their budget requests. They also must decide, given the amount of funding they have to work with, where tradeoffs have to be made, for example, should more be allocated to collection or processing? To personnel or investments in new technology?

Intelligence Programs Separately Funded by the Department of Defense

The NFIP budget at present comprises about two-thirds of the total spending for U.S. intelligence. The remainder is funded in one of two separate aggregations within DoD's budget:

- The Joint Military Intelligence Program (JMIP), managed by the Deputy Secretary of Defense, is composed of several separate sub-programs each managed by a different DoD official. They respond to defense-wide intelligence needs as opposed to the needs of a particular military service.
- Tactical Intelligence and Related Activities (TIARA) is an after-the-fact aggregation of funding for tactical military intelligence projects and combat support units which are not centrally managed. Within DoD, each military service and the U.S. Special Operations Command budget for its own tactical intelligence capabilities within the context of its annual budget. These decisions are reported to the Office of

the Secretary of Defense, which aggregates them for purposes of providing them to the Congress and others within the Executive branch.

In order to assess sensibly what should be spent on national intelligence programs funded in the NFIP, many of which principally support military requirements, the DCI and the NFIP program managers must understand which military intelligence capabilities are being separately funded by DoD in the JMIP and TIARA. Heretofore this was accomplished on a largely *ad hoc* basis, with the Assistant Secretary Defense for Command, Control, Communications and Intelligence (ASD(C^3I)) serving as the principal bridge between national, defense-wide, and tactical programs. Recently, however, the DCI and the Secretary of Defense agreed that all intelligence programs that support military operations would be reviewed together. After this joint review, the DCI and the Deputy Secretary of Defense would recommend an overall intelligence program and budget to the Secretary of Defense for his decision. The Secretary would then submit the defense budget, including intelligence funding, to the White House for inclusion as part of the President's budget.

The new joint budget review is clearly desirable to identify waste and duplication and improve overall efficiency among intelligence activities. However, some have urged the Commission to go further and recommend that JMIP and TIARA funds be consolidated with the NFIP. This one intelligence budget would be under the DCI's control to bring more coherence and efficiency to intelligence spending. The Commission does not, however, think that such consolidation is either necessary or desirable. DoD and its subordinate military departments have separate needs, apart from national needs, that they have a right—and indeed, an obligation—to fund. For example, the DCI is not the most appropriate official to decide how many (or which) reconnaissance aircraft are appropriate for Army units in Korea. This is not to say the military departments should act without regard to the overall needs of the nation, but only that they have separate needs which they attempt to satisfy within the funds available to them. The Commission's recommended changes to the budget process, described later, would effectively achieve the same result without unduly interfering with the independent authorities of the Secretary of Defense or those of the military departments.

The Commission also found numerous and significant shortcomings in the way the NFIP is structured and in the way it is prepared. The remainder of this chapter is devoted to these topics.

PROGRAM AND BUDGET STRUCTURE

Budgeting By "Business Area"

As noted above, the NFIP is composed of separate "programs," each with its own "program manager" (e.g. the Consolidated Cryptologic Program is managed by the Director, NSA). These component programs are not, however, grouped around a consistent organizing principle. Some fund a type of intelligence activity; others fund a particular agency; and others fund a combination of both. As a result, no single program manager has budgetary responsibility for a given intelligence "business area" or discipline (such as signals intelligence or imagery). Instead, activities within a particular discipline are funded in several component programs. In simple terms, like activities are not grouped together for purposes of resource allocation or program execution. This structure makes it very difficult to identify wasteful activities, decide where tradeoffs should be made, and determine where

cuts should be taken, if required. As the DCI recently observed, the "Intelligence Community has been relatively free from the systematic planning, programming, and budgeting process that is the hallmark of efficient government . . . The present system does not permit resource-saving trade-off analysis: for example, the possibility of substituting satellites for aircraft imagery or signals collection. . . ."

The existing structure also increases the likelihood that like activities funded in different programs will not interoperate or otherwise complement each other once deployed. The Commission was provided several examples by senior military officials and intelligence officers of redundant systems, funded in different programs, which were either inefficient or not interoperable. The problems with disseminating imagery during Operation Desert Shield/Storm, for example, were attributed to funding numerous imagery dissemination systems in different programs without coordination between them. Further, despite large expenditures on technical collection systems, the Intelligence Community's inability to process data collected by existing systems is attributable in part to the funding of these activities in different programs.

Given that like activities in each of the intelligence disciplines are also funded by DoD's JMIP and TIARA aggregations, and that the same situation exists with respect to each of them, the scope and effects of the problem are multiplied.

The commission concludes that the current program budget structure and diffused responsibilities over basic business areas have resulted in unnecessary duplication, interoperability problems, and other inefficiencies. These problems exist within the NFIP, and among NFIP, JMIP and TIARA activities, creating a substantial obstacle to the efficient use of intelligence resources.

7–1. The Commission recommends that:

(1) The budget for the National Foreign Intelligence Program be restructured by creating new discipline-oriented programs for SIGNIT, IMINT, MASINT and HUMINT, each with a single program manager (see Table 7.1 below). The budgets (but not operational control) for all SIGNIT activities in NFIP programs would be transferred to the new SIGNIT program; the budgets for all IMINT activities to the new IMINT program, and so forth. In addition to these discipline-oriented program budgets, the DCI should allow for agency-oriented infrastructure programs to fund activities that provide general support to the disciplines (e.g., CIA Headquarters building).

(2) The Secretary of Defense vest authority in the national program managers for SIGINT, IMINT, and MASINT, respectively, to perform the initial budgetary review of investments in defense-wide and tactical intelligence capabilities that may be funded outside of the NFIP. The Secretary of Defense would continue to have final approval on these DoD investment projects. The Director, NSA has already been placed in this position by the Secretary of Defense with respect to SIGINT activities. The Commission recommends extending this concept to the two other DoD officials who also would serve as national program managers. Each discipline or business area would then have a single authoritative program and budget manager for its intelligence activities. Responsibility for carrying out the various intelligence activities funded by any of these programs would not change under this proposal whether such responsibility now rests with national intelligence agencies or DoD elements.

The Commission believes that if these steps were taken, program managers would be able to develop cohesive programs involving all assets within a particular discipline, as well as trade off capabilities within a particular discipline (regardless of where the funds are

Table 7-1. Increasing Budget Formulation Responsibility for NFIP Program Managers in each of the Intelligence Disciplines

Intelligence Discipline	Proposed NFIP Program Manager	Percentage of *national* (NFIP) discipline activity budgeted by each program manager	
		Today	Commission's Plan
Imagery Intelligence	Director, National Imagery and Mapping Agency	3%	100%
Signals Intelligence	Director, NSA	52%	100%
Measurement and Signature Intelligence	Director, DIA	87%	100%
Clandestine Human Intelligence	Deputy DCI for CIA	96%	100%

Notes: Two proposed managers—the Director, National Imagery and Mapping Agency and the Deputy DCI for CIA—are positions which do not currently exist, but have been endorsed by the Commission.
The 3% figure, associated with imagery intelligence, refers to funds currently budgeted by the Director, CIO.
The 96% figure, associated with clandestine human intelligence, refers to funds currently budgeted by the Executive Director, CIA.

spent). These managers also would be able to better determine investment priorities, eliminate unwarranted duplication, and significantly improve end-to-end interoperability within their discipline.

These changes should also facilitate tradeoffs between disciplines, and between NFIP and Defense programs, substantially helping the DCI and the Secretary of Defense reach sensible, cost-effective decisions. They will also help OMB and the Congress perform their respective reviews and assessments of intelligence spending.

It was suggested to the Commission that intelligence budgets be constructed not around disciplines but around missions, e.g. support to military operations, support to policymaking, similar to the program "packages" used in the planning, programming, and budgeting process of the Department of Defense. The Commission agrees that examining tradeoffs among the various capabilities within each discipline (SIGINT, IMINT, etc.) in terms of how they satisfy mission categories is an effective way to make *program* decisions.

However, most intelligence capabilities can be used to support a variety of missions and the missions themselves are constantly in flux. It does not appear feasible, therefore, to build an intelligence *budget* according to how the intelligence capabilities being funded may or should be ultimately used. Clearly, those building intelligence budgets must understand the capabilities of the systems and activities being funded in terms of how well they can be expected to satisfy the requirements of a variety of missions. Moreover, once intelligence capabilities have been fielded, they must be managed in such a way as to achieve the missions of intelligence in the most efficient and effective way. (Thus, intelligence capabilities might be evaluated in terms of how they satisfy the requirements of

particular missions by arraying them on a matrix, with "missions" as columns and capabilities within "disciplines" as rows.) It is difficult, however, for the Commission to see how intelligence *budgets,* in the first instance, could be constructed according to particular missions.

Funding for Departmental Analysis in the National Foreign Intelligence Program

The NFIP includes three small programs[4] that fund the analysis of intelligence at the Departments of State, Treasury, and Energy. Each is developed within its parent department and competes against the other funding priorities of that department. After the Secretary of each department approves his or her proposed budget, including funding for intelligence analysis, the request is sent to OMB for review and adjustment in light of Presidential priorities.

Budget estimates for these intelligence elements also are sent to the DCI. But because the programs are small and have competed internally within their own departments, the DCI typically accepts the estimates without change.

The NFIP also includes the General Defense Intelligence Program (GDIP) managed by the Director, DIA. The GDIP funds an array of activities that provide for:

- military intelligence analysis at DIA, nine Unified Commands, and the military intelligence commands of the Army, Navy, and Air Force;
- infrastructure for DIA and the military service intelligence commands;
- intelligence openly collected by Defense Attaches and other DoD personnel;
- intelligence clandestinely collected by DoD personnel; and
- certain technical collection efforts (e.g. characterizing foreign nuclear testing).

Under the Commission's recommended structure for the NFIP, the GDIP's clandestine human intelligence activities and technical activities would be moved to the new consolidated national programs for clandestine human intelligence and measurement and signature intelligence, respectively. This would leave the GDIP composed essentially of intelligence activities that serve principally departmental purposes.

In light of this, the Commission considered whether the budgets for the small departmental intelligence elements and the reduced GDIP should remain within the NFIP. DCIs have historically played a limited role with respect to these budgets, but their budgetary role has been, and continues to be, a key element of their authority with respect to other elements of the Intelligence Community. ***To maintain the DCI's cognizance over these intelligence programs, the Commission concluded that the budgets for the small departmental elements and for the GDIP should remain under the DCI's authority as part of the NFIP.***

Counterintelligence Funding

As discussed in Chapter 2, counterintelligence is a critical part of nearly all intelligence activities. When performed properly, the counterintelligence function is integral

[4] As a group, these three programs constitute less than one-half of one percent of the NFIP.

to the intelligence activity itself and part of the overall security of the organization. As the Ames case demonstrated, the consequences of poor counterintelligence can be disastrous and deadly.

The FBI has a mission to "protect the U.S. from the intelligence activities of foreign powers and international terrorists through neutralization of activities inimical to our national security interests." By law and Presidential directives, the FBI has been designated as the federal government's lead agency for counterintelligence investigations and operations. Outside the U.S., the FBI coordinates its counterintelligence efforts with the CIA. Within other elements of the Intelligence Community, counterintelligence principally involves providing internal security to the parent organization at a level consistent with the needs of the organization.

Given these factors, the counterintelligence function is not readily amenable to budgetary tradeoffs among the various agency counterintelligence staffs. There is, however, a need for an independent review of counterintelligence budgets to ensure that adequate resources are being allocated to the function consistent with national objectives and priorities. In the past, funding for counterintelligence activities has occasionally been a convenient place for agencies under budget pressures to find money for other activities. This must be assiduously prevented. Funding for counterintelligence activities is now provided by the NFIP subject to the DCI's approval. Separate authority to conduct reviews of counterintelligence budgets is also lodged by Presidential Directive in the National Counterintelligence Policy Board, created in 1994 in the wake of the Ames case. The Board reports to the Assistant to the President for National Security Affairs and includes senior representatives from the FBI; CIA; the Departments of Defense, Justice, and State; the military services; and the National Security Council staff.

The Commission believes that funding for counterintelligence activities should remain a part of the National Foreign Intelligence Program. At the same time, it is useful to have the National Counterintelligence Policy Board perform a separate review of counterintelligence budgets. Together, they should provide assurance that funding is adequate to achieve national objectives and priorities as well as prevent counterintelligence funds being used for other purposes.

THE BUDGET PROCESS

In addition to the problems found in the existing budget structure, numerous problems appeared to exist with the process used to develop and implement the budget.

Program Guidance and Evaluation

The DCI is charged by law to "provide guidance to elements of the Intelligence Community for the preparation of their annual budgets."[5] Usually, this guidance is issued by the DCI's staff or jointly with the Office of the Secretary of Defense after an overall level of funding has been decided by the Secretary of Defense and the DCI, and takes into account presidentially directed needs and priorities, statements of national security strategy, analyses of intelligence "gaps" and future needs, and other pertinent direction. Often, however, this guidance comes after the program and budget process has begun, and the program

[5] Public Law 102–496, Sec. 705.

managers have already incorporated their own assumptions about intelligence requirements into budget estimates. In the view of the Commission, the current quality and timeliness of program guidance is far from optimal.

Furthermore, according to many who spoke with the Commission, it is rare, if ever, that a program manager will have adequate evaluations from customers of how well the activities funded by his or her program respond to their information needs. Without such evaluations, it is difficult for program managers to identify and give priority to their most effective intelligence capabilities when building programs.

On the whole, the Commission believes that evaluations of intelligence by users should be relied upon to a far greater extent in the budget process. In Chapter 3, the Commission recommends that a "consumers committee" be established as part of a "Committee on Foreign Intelligence" under the National Security Council with ongoing responsibility to identify intelligence requirements and priorities, and to evaluate the Intelligence Community's response to policymakers' requirements. Inputs from this Committee, along with the fiscal decisions which he develops with the Secretary of Defense, should help the DCI to issue effective and timely guidance to support program and budget building. These evaluations also should enable program managers to know what intelligence support is, and is not, working well.

Strengthen Community-Wide Analysis of Intelligence Budget Items

Historically, the program and budget submitted by each NFIP program manager has been changed little, if at all, by the DCI's staff. There are several reasons for this, including the lack of a sufficiently capable analytical staff permanently assigned to the DCI, the DCI's focus on other important responsibilities, and prior agreements between the DCI and DoD which excluded certain staff offices of the Secretary of Defense (e.g. Comptroller and Program Analysis and Evaluation) from reviewing NFIP programs, as they do for Defense programs. In the view of the Commission, these bureaucratic arrangements must be changed if economy and efficiency are to be achieved. While the new DCI has taken initial steps in this regard, they have not yet been implemented fully.

7–2. The Commission recommends that the DCI establish a permanent cadre of analysts reporting to the Deputy DCI for the Intelligence Community to analyze and evaluate intelligence programs, identify inefficiencies within those programs, and assess trade-offs among programs. These analysts should include some with experience in the intelligence agencies and some with experience principally outside of intelligence. Further, current plans to include the DoD Comptroller, the Secretary of Defense's Program Analysis and Evaluation staff, and OMB staff in the review of national intelligence programs should be carried out.

Information on intelligence programs has not been organized to facilitate decision-making by the DCI or to provide outside reviewers, such as OMB, with an informed view. Although the DCI and DoD each maintain classified databases that track intelligence resources, they do not allow decisionmakers to have their questions readily answered at a meaningful level of accurate detail. Furthermore, 60 percent of NFIP funds are obscured by lumping them into a category called "base" which is minimally described, even in budget books sent to the Congress. It is these types of vague accounting and budgeting practices that permitted the accumulation of large NRO reserves, reported recently in the media, to go undetected.

The Commission understands that commercially-available computer technology would permit existing agency data files to be aggregated and analyzed without re-keying or manually re-formatting the data, allowing for the creation of a consolidated Community-wide data base that encompasses national, defense-wide, and tactical resources. However, despite the power of available technology, implementing this management information system may require one to two years to achieve the desired results.

Ideally, the building blocks of such a database would be individual "projects" or "activities" that accomplish a single purpose, rather than large amounts attributed to "base" that do not inform decisionmaking. Such a change would be in line with the private sector trend toward "activity accounting" to improve decision-making.

In the Commission's view, a Community-wide database of national, defense-wide, and tactical intelligence resources is feasible and highly desirable. Such a tool would allow the Secretary of Defense, the DCI, program managers, and other stakeholders to identify program issues, analyze all related resources, and improve the chances for implementing the most cost-effective intelligence program. An improved budget process, as recommended above, should allow the DCI and Secretary of Defense to identify excesses or shortfalls within each intelligence discipline and facilitate tradeoffs among the intelligence disciplines to optimize the government's intelligence posture. For example, the DCI and Secretary would be able to track funding for new technological innovations regardless of program and funding source. Better and more accessible resource data would allow program managers to design and fund a more efficient end-to-end system for each intelligence discipline and facilitate a matrix approach to budget analysis that would allow program managers to evaluate how particular intelligence capabilities were contributing to the missions of intelligence.

7–3. The Commission recommends that the DCI, in consultation with the Secretary of Defense, develop and implement a database to provide timely and accurate information on the purposes, amounts, and status of resources for national, defense-wide, and tactical intelligence activities. To minimize time and expense, this database should build upon existing data files from the agencies involved and be available for use by all appropriately cleared resource management officials and decisionmakers. A goal should be established to have such a database in place prior to developing the budget for fiscal year 2000.

Monitoring Expenditures

In the normal course of the budget process, once Congress authorizes and appropriates funds, OMB apportions the funds to DoD for all programs included in the DoD budget. The DoD Comptroller then transfers to the military services, defense agencies, and the CIA the authority to spend money in accordance with the congressional direction. In turn, the agencies build their financial plans and display in detail the manner in which they intend to spend money. Deviations from these plans that exceed stated thresholds are subject to "reprogramming" actions, usually requiring the approval of Congressional committees, the DCI, the Office of the Secretary of Defense and OMB. The DCI, program managers, and other review authorities must remain apprised of the status of expenditures in order to ensure that programs are being implemented according to the intent of the original requests and Congressional mandates. Currently the DCI must be notified by agencies of reprogramming actions that exceed Congressional thresholds. ***The Commission found that the***

DCI and his staff, some program managers, and other review authorities such as OMB, are not always given sufficiently detailed information to stay abreast of how agencies are spending money. Knowledge of current spending in any one area is critical to formulate and review requests for new spending in that area.

7–4. The Commission recommends that all intelligence agencies provide the DCI, program managers, and other review authorities with budget execution (spending) reports in sufficient detail to follow budget implementation and analyze reprogramming requests. The budget spending reports should be periodic, timely, and at a meaningful level of detail (e.g. by major project).

THE IMPACT OF THE COMMISSION'S RECOMMENDATIONS

The Commission believes that if the recommendations proposed in this chapter are adopted, they would provide a far more effective framework for the allocation of intelligence resources. They would facilitate the identification of wasteful activities, promote interoperability among systems and programs, and provide a better basis for streamlining and consolidation. The public would have greater assurance that the Intelligence Community of the future was operating effectively and efficiently. The budget structure and process which exist today do not provide such assurance.

The Commission's recommendations on the budget process, particularly building a Community-wide resource data base, would require an initial (though not large) outlay of funds, but should pay for themselves many times over in terms of the efficiency brought to the budget process.

IMPROVING INTELLIGENCE ANALYSIS

The *raison d'etre* of the Intelligence Community is to provide accurate and meaningful information and insights to consumers in a form they can use at the time they need them. If intelligence fails to do that, it fails altogether. The expense and effort invested in collecting and processing the information have gone for naught.

Assessing how well the Intelligence Community accomplishes this fundamental task is a complicated matter. A great deal of analysis is published; much of it is timely and of excellent quality. The Intelligence Community has many analysts who are recognized experts in their respective fields and whose professional judgments are valued and relied upon. Clearly, intelligence analysis has substantial value to many consumers.

The Commission found especially close ties between the producers and users of military intelligence. Within the military there is a long history of respect for, and reliance upon, intelligence. Intelligence is factored into strategic and tactical planning, is exercised in war gaming, and is integral to operations. As a result, military requirements are better defined, in large part, because of the close and continuing dialogue between intelligence analysts and the military commands they support.

Where policy agencies are concerned, however, consumers more often take a jaundiced view of the analytical support they receive. The President and senior cabinet officials appear to be relatively well served, but many decisionmakers at lower levels find that intelligence analysis comes up short. Often what they receive fails to meet their needs by being too late or too unfocused, or by adding little to what they already know.

In fact, only a small percentage of the resources allocated to intelligence goes to "all-source" analysis. Relatively few resources are devoted to developing and maintaining expertise among the analytical pool. Intelligence lags behind in terms of assimilating open source information into the analytical process, and it continues to struggle with how to avail itself of expertise in the private sector. Analysis that is not responsive to consumer needs continues to be produced.

The Intelligence Community is not entirely to blame. Consumers have a responsibility not only to engage in the process but, more important, to drive it. Often, they are uncooperative or too busy to engage at all. Since most are political appointees, many enter and leave government never appreciating what intelligence might have done for them. Clearly, consumers need to be better educated about the value of intelligence.

The Commission did find numerous instances where there was a close working relationship with policymakers. Intelligence producers were able to focus on issues of significance and to make information available when needed. Analysts understood the consumer's level of knowledge and the issues he or she wanted help on. Their analysis was read and relied upon. The consumer, for his part, developed an understanding of what intelligence could do for him and—equally important—what intelligence could not do. Many considered the support vital to meeting their responsibilities and actively engaged in
[still-classified section missing here]
[still-classified section missing here] has no capability of its own to collect or to analyze information. While the United States presently provides the majority of the information that the UN receives in support of its operations, this support remains relatively limited. Other nations reportedly contribute very little.

In general, the Commission believes the United States should use its broad experience in intelligence matters to arrange for appropriate information support to multinational

bodies as well as international coalitions, where important interests of the United States are at stake. The Commission is persuaded that this can be accomplished without jeopardizing the security of U.S. intelligence activities. It may require "sanitizing" information produced by intelligence agencies to ensure protection of sources or methods and/or limiting this sanitized information to particular topics or operational activities. These actions do place extra burdens on U.S. intelligence agencies to assess the particular needs of foreign recipients, to create "sanitized" versions of their reports, and to set up separate dissemination channels and/or communication systems for the foreign recipients. But, in the Commission's view, it is essential that the effort be made. Good information support is ordinarily critical to the success of any multilateral or coalition operation in which the U.S. is involved and, as a practical matter, the United States may be best positioned to take a leadership role.

In providing such support, U.S. intelligence agencies ordinarily should not deal directly with multinational organizations or coalitions, but rather should work through other elements of the U.S. Government (e.g. the Department of State for diplomatic actions, appropriate military channels for military coalitions). The U.S. agency charged with overall responsibility for the relationship with the multinational organization or coalition being supported will usually be in the best position to understand the needs of the recipients and balance risk versus gain.

The Commission's impression is that the arrangements for information support to multinational organizations or coalitions are often constructed and tailored to meet particular situations. While a certain amount of tailoring will inevitably be needed for each organization or coalition supported, new policies, procedures and capabilities (e.g. communications systems) should be developed to provide the standard means and methods for providing support in a multinational environment, similar to those in existence with NATO. Deviations could be authorized as appropriate.

12–1. The Commission recommends that the DCI and the Secretaries of State and Defense jointly develop a strategy that sets forth the policies, procedures, and capabilities that will normally serve as the basis for sharing information derived from intelligence in a multinational environment as well as how deviations from these policies, procedures, or capabilities may be authorized. To achieve maximum effectiveness, this strategy should build upon the extensive set of bilateral and multilateral relationships already maintained by the United States.

THE COST OF INTELLIGENCE

Viscerally, in the wake of the Cold War, many Americans believe the costs of intelligence should go down. Indeed, since 1989, the resources allocated to intelligence have gone down—by about 21 percent in real terms—but, nonetheless, they remain substantial. Budget projections show spending for intelligence holding relatively constant in real terms through the rest of the decade. Reflecting a sense of unease, Congress asked this Commission to determine "... whether the existing levels of resources allocated for intelligence collection and intelligence analysis are seriously at variance with United States needs. ..."

To answer this question, the Commission undertook an extensive review of the intelligence budget and analyzed the changes to that budget since 1980. In doing so, the Commission attempted to ascertain what basis, if any, had been used over time to arrive at the resource level for intelligence. Was there a discernable standard or criteria that might help those responsible for resource allocations in the future to determine how much intelligence is enough?

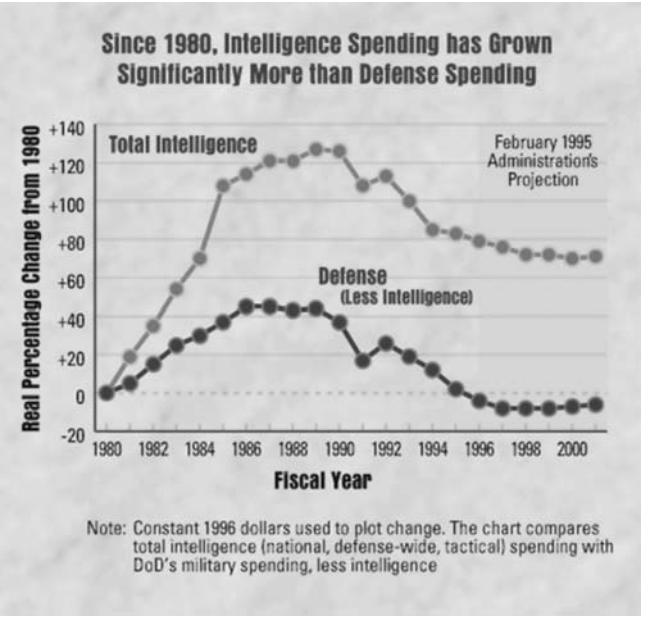
Recognizing that pressure to reduce spending is apt to continue, the Commission attempted to assess whether and how the costs of the existing intelligence capability could be reduced without damaging the nation's security.

The Recent History of Intelligence Funding, in Brief

In recent decades, intelligence funding has been treated preferentially when compared to other parts of the Defense budget. As Figure 1 illustrates, non-intelligence defense funding in real (constant dollar) terms grew by 40 percent from 1980 to 1986, leveled off, and then declined to its current level, four percent below its 1980 level. In contrast, total intelligence funding grew by 125 percent in real (constant dollar) terms from 1980 to 1989 but declined thereafter to its current level of 80 percent above 1980. Reductions taken in the intelligence budget since 1989 have been at a rate to allow the intelligence agencies to continue most of their basic activities. Each agency has taken its share of the reduction from 1989, but no major structural change was required.

Personnel strength at NSA, CIA, and DIA has also remained significantly above the 1980 level despite across-the-board reductions over the last four years. NSA is 22 percent above its 1980 level; CIA, 8 percent; and DIA, 80 percent, primarily because DIA assumed major new functions which involved the transfer of additional personnel. In 1991, Congress in concert with the Bush Administration imposed a 17.5 percent across-the-board reduction in intelligence personnel to be accomplished between 1991 and 1997. This is less than 3 percent per year and has already largely been accomplished through attrition. This agreement had the Intelligence Community already on track when President Clinton directed that overall government personnel be reduced by 12 percent from 1993 to 1997, or about 3 percent per year. The Community has, in fact, extended these reductions through 2001, resulting in an anticipated total reduction from 1991 to 2001 of about 24 percent. This pace of reduction is consistent with the level of reductions that the President has directed for non-intelligence agencies.

Although intelligence funding remains classified, Figure 2 depicts the relative funding levels of the major intelligence agencies and their personnel levels for FY 1996. NSA, CIA, and DIA (and the Service intelligence units) have the largest number of personnel; the NRO, on the other hand, has the highest level of funding of any program in the Community,



but virtually no federal workforce. Its work is accomplished primarily by contractors in the private sector.

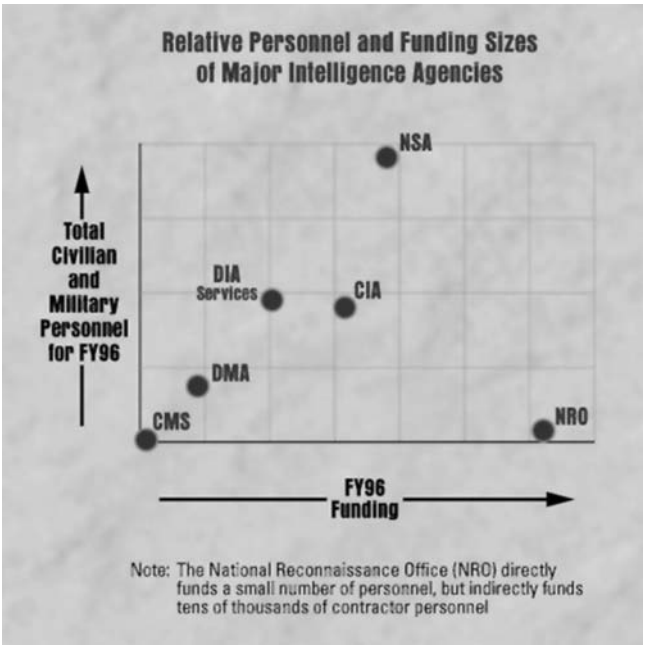
The Community Management Staff (CMS) is the small staff of the DCI used to assist in the execution of his Community functions.

What Conclusions Can Be Drawn from Recent Experience?

In general, from 1980 until the present, intelligence grew at a faster rate than defense when defense spending was going up and decreased at a slower rate when defense spending was going down. As a result, intelligence funding is now at a level 80 percent above where it was in 1980, while defense overall (other than intelligence) is now 4 percent below its 1980 level.

Because the Secretary of Defense in consultation with the Director of Central Intelligence has largely determined[1] the size of the annual budget for intelligence vis-à-vis the remainder of the defense budget, one conclusion that might be drawn is that successive Secretaries since 1980 have believed that intelligence should be funded at a somewhat higher rate than defense (regardless of the rate of increase or decrease for defense as a whole). Based upon the Commission's interviews, it appears that, in practice, most Secretaries have begun with the amount appropriated for intelligence the previous year, taken into account whether the overall defense number is increasing or decreasing, examined the additional initiatives needed for intelligence, and arrived at a somewhat preferential number for intelligence spending. Compounded over a period of years, this practice has led

[1] Congress annually makes adjustments to the President's budget request.



to the relatively large disparity between where intelligence is now funded, relative to its 1980 level, as compared with where defense spending other than intelligence is now funded relative to its 1980 level.

The Commission does not conclude the practice followed by successive Secretaries of Defense is necessarily right or wrong, but only that it has been the case. Nor does the Commission conclude that the wide disparity between intelligence spending and defense spending, relative to their 1980 levels, necessarily means that intelligence spending should be cut. But what, then, should be used to gauge the level of spending for intelligence?

The Commission struggled to find a substantive standard or criteria that might serve as a basis for answering this question. Some suggested that the spending level for intelligence should be what is needed to support the military operational requirements of a particular Administration, e.g. the "two major regional conflicts" strategy of the current Administration, and all other intelligence needs should be met by the same intelligence capabilities. The capabilities needed to support military operations, however, will not satisfy all intelligence needs. For example, the President and other users (including defense officials) rely on information produced by intelligence capabilities that are not principally used to support military operations, e.g., HUMINT, some imagery, and some signals intelligence activities. Moreover, the operational needs of the military provide no real limits to intelligence spending. As military commanders seek to win battles while minimizing casualties by knowing where the enemy is at all times—what the Pentagon has been referring to as "dominant battlespace awareness"—the need for intelligence grows exponentially. The costs of collecting signals and imagery intelligence from satellites, processing it at ground stations, and transmitting it to foxholes, tanks and aircraft in the "battlespace," all in

a matter of seconds, are potentially unlimited and, regardless of how much capability is available, it may never provide total coverage.[2]

The Commission found it is equally difficult to assess the overall resource level for intelligence based upon the perception of the "threat" at any given point in time. If one target is no longer considered a "threat," intelligence collectors usually can be moved to others that are. Indeed, since intelligence collection capabilities, both human and technical, take years to deploy once resources for them have been provided, they are designed to be flexible in order to adapt to new needs.

Ultimately, the Commission concluded that developing a precise criterion for measuring the right level of intelligence resources would inevitably be too simplistic and perhaps unwise. The reality, as for many functions of government, is that intelligence capabilities are determined by whatever the nation chooses to spend on them, not by some rigorous calculation which attempts to precisely balance threats against capabilities. Like the conduct of diplomacy, controlling commercial air traffic, monitoring weather, or defending our borders, there is always more that could be done. Unlike the precision that the government can attach to the cost of delivering a letter, or printing and delivering a Social Security check, there is no precise means to determine how much the nation should spend on intelligence. Just as with other aspects of our national security, determining the appropriate level for intelligence funding requires an assessment of various criteria such as foreign threats and the advantages a particular capability can provide against such threats. These must then be weighed against what the nation can afford, given other government spending requirements and priorities.

In any event, how much the nation can afford to spend on intelligence has been and will continue to be constrained. While the need for such capabilities is compelling, so too is the need to reduce Government spending. Over the next decade, there is likely to be strong and persistent pressure to reduce the costs of Government across the board. Given the fact that the President and the Congress have now agreed in principle to balance the federal budget by the year 2002, deficit reduction casts a particularly long shadow over future intelligence investments. Though the calculations thus far agreed upon for balancing the budget assume that defense spending is capped and intelligence funding remains flat within this cap, changes in the economy or other spending priorities could re-open the debate on the level of spending for defense and hence impact intelligence. Therefore, reducing intelligence funding due to external pressures may be unavoidable in the long run. Furthermore, internal Defense Department pressures to reduce intelligence are also growing as the military services vie for funds to modernize their forces, maintain current levels of readiness, and pay for an increasing number of peacekeeping missions. Even within the existing cap for intelligence in the projected budget, there will be pressures to hold costs down in some areas and increase them in others.

What Needs to be Done

In view of these pressures, it behooves those with responsibility for intelligence resources to begin planning how such resources might be further reduced and/or reallocated

[2] There is, in fact, a process within DoD for trading off intelligence expenditures needed for the support of military operations against non-intelligence expenditures needed to support military operations within the overall limits of the DoD budget. Support to military operations does provide, in any case, the principal justification for the overall level of expenditure for intelligence within DoD.

to meet future intelligence requirements. Unfortunately, while the Commission found evidence of such planning in a few agencies, most intelligence agencies seemed to lack a resource strategy apart from what is reflected in the President's current six-year budget projection. Indeed, until the Intelligence Community reforms its budget process, it is poorly positioned to implement such strategies. The Commission's recommended actions to improve the budget process, set forth in Chapter 7, are thus a necessary first step towards more rational resource planning. The Commission also believes that certain of its other recommendations, if implemented, would produce costs savings:

- The one-time personnel authority outlined in Chapter 9 to "rightsize" to meet the needs of the Intelligence Community could save an estimated $2–3 billion in personnel costs over a ten-year period.
- The infrastructure costs associated with maintaining the existing level of personnel (e.g. buildings, communications, recruitment, security, training) could also be reduced, as noted in Chapter 9.
- Increased international cooperation in space reconnaissance, as recommended in Chapter 11, could, in time, also achieve savings.

In addition, there are a number of developments external to the Intelligence Community which offer promise of cost reductions:

- Aggressive implementation of the acquisition reforms recommended by the Defense Science Board would reduce the burden on industry and government of excessive red-tape and unnecessary oversight, and should reduce the costs of contract administration for most DoD intelligence components;
- Capabilities under development in the private sector, such as commercial imaging systems, might prove sufficiently reliable that intelligence capabilities could be reduced; and
- Potential savings could also stem from greater use of commercial technology for intelligence purposes, such as using commercial communication systems to disseminate intelligence to consumers around the world.

The Commission also explored the feasibility of reducing costs by allowing intelligence agencies to charge their consumer departments and agencies for the support they receive. Many witnesses pointed out that intelligence is a "free good" to most departments and agencies. Whether the support provided by intelligence is a map for a State Department analyst, an intelligence report on the economic conditions in a particular country for a Treasury analyst, or imagery necessary for precisely targeting Air Force cruise missiles, the cost of producing these intelligence products is free to the user. Because it is free, the appetite of consumers is essentially insatiable and undisciplined. Consumers who appeared before the Commission conceded that if they had to pay for intelligence support out of their agency budgets, they would, in fact, be more judicious in the number and type of requests they levied.

While charging for intelligence support may, indeed, bring greater discipline to the system, the Commission found many practical difficulties in implementing such a system. One is assigning cost to intelligence support. How does one assign a monetary value to an intelligence analysis, or a map, or a photograph? Another is providing intelligence support to departments and agencies who need it but have not asked for it. What do intelligence

agencies do when they have crucial information for a particular department or agency, but the customer agency has used up its annual allocation for intelligence support? How would such a system be administered? Would each intelligence producer keep its own accounts? Would departments and agencies who were delinquent in their payments have their intelligence spigots turned off?

The Commission concluded that the benefits of bringing greater discipline to the current system by permitting intelligence agencies to charge for their services were far outweighed by the difficulties apparent in implementing such a proposal.

The Commission did, however, make one additional effort to assess intelligence costs by undertaking a review of the projected budget for intelligence from FY 1996–2001 in order to ascertain whether there appeared to be intelligence programs that were duplicative or providing marginal value. The conclusions of this review are set forth in the next section.

THE COMMISSION'S BUDGET REVIEW

The purpose of the Commission's review was to determine whether there were existing intelligence capabilities, developed during the Cold War, which appeared to be duplicative of each other or of other government capabilities, or which otherwise provided capability excess to the country's needs in the post-Cold War era. The intent of this review was not to arrive at recommendations for cuts to specific programs, but rather to judge whether such problems were apparent, and, if so, to what extent.

To perform this review, the Commission's staff organized the President's FY 1996 to FY 2001 budget for national and tactical intelligence programs into seven "business areas:" 1) signals collection and processing, 2) imagery collection and processing, 3) human source collection and processing, 4) measurement and signature collection and processing, 5) production and analysis of intelligence products, 6) multidisciplinary intelligence (those programs that contribute to multiple intelligence disciplines), and 7) intelligence infrastructure (buildings, support staffs, telecommunications, etc.). All intelligence programs and activities funded by the National Foreign Intelligence Program, the Joint Military Intelligence Program, and the Tactical Intelligence and Related Activities aggregation were included.

Within each of the business areas identified above, further divisions were made to identify the end use, target, or ultimate purpose of the expenditure. For example, the business area of "imagery collection and processing" was divided into three further categories: 1) imagery of the battlefield; 2) imagery for indications and warning intelligence, science and technological developments, and other needs; and 3) imagery management and dissemination. The purpose of this approach was to align expenditures for intelligence programs with their ultimate purpose or target in order to make informed decisions concerning possible duplication or excess capability.

Ultimately, the Commission staff assessed the contributions made by each intelligence program or activity with respect to each of the selected end uses or targets, and judged whether the programs were appropriate given the end of the Cold War, whether they duplicated other programs, and whether they provided excessive capability. These were necessarily subjective judgments based upon the staff's appreciation of the Government's need and what the respective programs and activities contributed in particular areas.

The Commission nonetheless believes the staff's review demonstrated that reductions to the existing and planned intelligence resources may be possible without damaging the nation's security. Indeed, finding such reductions is critical if funds are to be

found for the investments in intelligence capabilities that the nation will need in the future, capabilities that are not now funded in the proposed program and budget. Precisely where such reductions should be made and at what level are judgments which the Commission is not in a position to make. Nonetheless, it is clear a more rigorous analysis of the resources budgeted for intelligence is required. In the Commission's view, this analysis should be performed jointly by the DCI, the Secretary of Defense, and the Director, OMB. It should span all three sources of intelligence funding (NFIP, JMIP, and TIARA) and assess the total U.S. intelligence capability against particular targets or types of targets.

In sum, the Commission believes cost savings can be achieved if the Intelligence Community adopts the management practices and implements the cooperative arrangements summarized earlier in this chapter. Those actions, together with pruning unnecessary requirements and unproductive systems and activities, could free significant resources. At the same time, the Commission recognizes that its proposed reforms to the budget review process could result in the identification of shortfalls between programmed resources and needed capabilities, or identify areas where new developments and investments are needed but are not now programmed. This might require the expenditure of most, perhaps all, of the funds freed up by cost saving measures. The Commission itself is not in a position to make this assessment.

APPENDIX H

REMARKS ON INTELLIGENCE OVERSIGHT, DCI ROBERT M. GATES, 1993

AMERICAN INTELLIGENCE AND CONGRESSIONAL OVERSIGHT

Today marks the last speech that I will give as Director of Central Intelligence. I have decided to use this opportunity to talk with you about Congressional oversight of intelligence and how it can be strengthened.

The idea of Congressional oversight of intelligence first came up a year after CIA was created by the National Security Act when, in 1948, there was a motion to establish a joint committee to oversee intelligence. This motion, which failed to get out of committee, was the first of nearly 150 proposals concerning intelligence oversight that would follow over the next 25 years. Just two of those proposals made it to the floor for action and both were defeated by greater than 2 to 1 margins.

Not that CIA was totally without Congressional oversight in the first quarter century of its existence. The Armed Services Committees and Defense Subcommittees of the Appropriations Committees had authorizing and appropriating jurisdiction for the Intelligence Community.

However, there were never more than a few Members of either House that actually participated in this oversight of intelligence. The number of hearings was limited and, according to one expert on Congress and intelligence, there were several years where the Senate oversight bodies met only once or twice.

By the early 1970s, the Director or Deputy Director averaged some 30 to 35 committee

---

Source: Remarks by Robert M. Gates, Director of Central Intelligence, Before the World Affairs Council of Boston, Massachusetts (January 15, 1993), reprinted in "Legislative Oversight of Intelligence Activities: The U.S. Experience," *Report,* S. Prt. 103–88, Select Committee on Intelligence, U.S. Senate, 103d Cong., 2d Sess (October 1994), Appendix 10.

appearances annually. There were even briefings for the Congress on covert action. For example, Foreign Relations Committee Members were briefed as early as 1962 on covert assistance to the Myong in Laos and during the ensuing years Foreign Relations and Armed Services Committees of the Senate were briefed on a total of 28 occasions on this effort alone.

Even so, Chairman of the Intelligence Subcommittee of the House Armed Services Committee Lucien Nedzi accurately described the overall state of Congressional oversight in a talk to the CIA Senior Seminar in November 1973, when he said, "It is a sobering experience for me, as Chairman of the House Intelligence Subcommittee, to find our Subcommittee still in the process of defining ourselves, still exploring (or worse yet, just beginning to explore) what we can do and what we must do."

The pattern of oversight just described was not a product of CIA or Intelligence Community reluctance to appear before the Committees or inform the Congress. The Subcommittees were regularly informed of the most significant covert programs and routinely briefed on the intelligence budget. As one observer put it, "The mechanism for oversight clearly existed; what was missing was an interest in using it—or more properly speaking, a consensus that would legitimize its use."

By the mid-1970s, a broad consensus emerged for the creation of a permanent and more effective Congressional oversight capability. Both the Rockefeller Commission and the Church Committee separately recommended creation of committees to oversee intelligence, and those recommendations were enacted into law by the Senate in May 1976 through Senate Resolution 400. The House acted a little over a year later in July 1977 with House Resolution 658.

In the early 1980s, Congress demonstrated its support for good intelligence and also its interest in stronger oversight both with support for increased funding and with three major pieces of legislation affecting intelligence. First was the Classified Information Procedures Act that provided for the protection of classified information—especially intelligence information—in courtrooms. Second was the Intelligence Identities Protection Act. Following the assassination of CIA Station Chief Richard Welch, the Congress moved to make it illegal to publicly identify a CIA officer who was under cover.

Finally, and most significantly, the Intelligence Oversight Act of 1980 reduced the number of Committees overseeing the Intelligence Community from eight to two—the Select Committees of the House and Senate, but also established certain obligations on the part of CIA and the Intelligence Community: to keep the Committees fully and currently informed of all intelligence activities, to furnish information deemed necessary by the Oversight Committees, and to report illegal or failed intelligence activities in a timely fashion. The legislation also revised the notification procedures for covert action, again reducing the number of Committees notified from eight to two.

So where do we stand today? Over the past sixteen years, CIA accountability and legislative oversight have grown enormously. With this oversight, CIA and the other intelligence agencies have become the most scrutinized intelligence services in the world. It would be difficult for any secret intelligence organization to be placed under this microscope of intense review. And yet, I believe, under these circumstances we not only remain effective and capable, we enjoy a legitimacy and an acknowledged role in our government not shared by any foreign intelligence service. It is fair to say today that there is not a single planned or ongoing activity in the Intelligence Community that it is not in some way or another subject to review by at least two Committees of the Congress.

To give you some insight into the breadth of this relationship, let me cite a few statistics. In 1992, representatives of the agencies of the American Intelligence Community met more than 4000 times with Members and staff of the Congress in either briefings or other meetings. We provided over 50,000 documents to the Congress and responded to almost 1200 questions for the record or Congressionally-directed queries.

Now, let me address two areas of special interest to Congress. First, the budget. The Intelligence and Appropriations Committees of the House and Senate take seriously their oversight responsibility to review the Intelligence Community budget and examine planned intelligence expenditures into the billions of dollars. They scrutinize budget line items in the thousands. In so doing, they pass judgment on virtually every plan and program. And Congressional oversight of the intelligence budget does not end after funds have been appropriated. We must gain the approval of up to six Congressional Committees when we reprogram money beyond a minimal amount and we must notify four Congressional Committees of any withdrawal of money from the CIA's reserve fund for contingencies. Furthermore, both intelligence authorizing committees and the House Appropriations Committee have created their own audit units and these have access both at Headquarters and in the field to our books and our expenditures.

The second area of special interest to Congress is covert action—actions which support the foreign policy objectives of the United States but cannot be achieved by overt means. The United States has the most elaborate set of checks and balances on its covert activities of any country on earth.

Few realize that most covert action proposals originate in the National Security Council or the State Department. But before any proposal for covert action moves forward, it is subject to intense scrutiny inside the CIA. The Covert Action Review Group—which includes the Executive Director of the Agency, the four Deputy Directors, the General Counsel, the Directors of Congressional and Public Affairs and the Comptroller—examines the critical legal issues of the covert action and also asks an important question: "If this program becomes public, will it make sense to the American people?"

Under the laws governing the oversight of intelligence, covert actions are conducted only after the proposal has been reviewed and approved by the National Security Council, the Attorney General, and finally, the President. The President's approval is embodied in a written Presidential Finding—which explicitly acknowledges that this operation is important to the national security of the United States. For the last seven years, every finding has been briefed to the Congress within 48 hours of signature.

The intelligence committees hold hearings to review new covert actions approved by the President, and they regularly examine all on-going actions. These two committees not only know the nature of the covert action that we are undertaking, but they know exactly how we are doing it, and they monitor every dime that is spent on it. This is no pro forma exercise. Congress can—and has—exercised control over CIA covert actions by denying us the funds needed to carry them out—just as it approves funds for all covert action that are undertaken.

Contrary to the image sometimes portrayed, most American intelligence officers welcome Congressional oversight—and all are subject to it. We see these Congressional mechanisms as surrogates for the American people, ensuring that our intelligence services operate within the law but also in ways consistent with American values. Congressional oversight is a protection against misuse of the Agency by Executive authorities and Congressional review of our intelligence publications helps guard our objectivity. Intelligence

professionals believe that effective oversight is vital if intelligence is to have a future in this most radically democratic country in the world.

The vast majority of CIA employees have grown up under Congressional oversight. More than 75% of the Agency's population has entered on duty since the creation of the oversight Committees. They understand the rules and appreciate the value of and reasons for oversight.

Having said that, the process by which American intelligence agencies became accustomed to and positive about Congressional oversight was a long, and often difficult, one. Especially in the first half of the 1980s—and occasionally afterward—there were periodic crises of confidence brought on by concern on the part of the Oversight Committees that they were not being dealt with candidly, in a full and forthcoming manner. These concerns were too often justified, at least in some measure. However, in recent years the relationship between American intelligence and the Congress has improved steadily to reach its current excellent state.

Yet, just as we have focused in recent years on improving our performance in this relationship, today I would like to reflect from our perspective on several problems on the Congressional side which, if addressed, could strengthen and enhance oversight while contributing to the further improvement of our intelligence.

My first and most important concern is that very few Members of the Intelligence Oversight Committees (or the Appropriations Committees) appear to devote much effort or time to their intelligence oversight responsibilities. Only a handful of Members in both Houses have taken the time to visit the intelligence agencies and to make the effort required to gain some knowledge and understanding of what is a very complicated and sophisticated undertaking. This places an enormous burden on the Chairmen and Ranking Minority Members. Individual Members from time to time will develop an interest in one or another aspect of our work and acquire some knowledge of that, but the number of those with broad understanding and real knowledge in my judgment can be counted on the fingers of one hand—and that is after 15 years of continuous oversight. At the same time, there are too many instances of members of our committees having important misunderstandings, misconceptions or just wrong facts about U.S. intelligence, including their own legislation governing our activities.

Most Members of Congress are among the hardest working people I have ever met. But they have many Committee assignments, must carry out their responsibilities to constituents, and they have a multitude of other obligations. The sad result is that Committee hearings and briefings are usually not well attended and it is my experience that the record is getting worse, not better.

Let me give you one example. We had a single budget hearing for Fiscal Year 1993 in the Senate Intelligence Committee last spring. The heads of all of the intelligence agencies were present. Of the 15 Members of the Committee, the Chairman and a handful of members, perhaps three or four, showed up. A half-hour or so into the hearing, it was recessed for a vote and when the hearing resumed a short while later, the Chairman and only two or three members returned. All but the Chairman were gone within 20 minutes. The result is that for the single most important hearing of the year—on the budget of the entire Intelligence Community—only Chairman Boren was present throughout.

By the same token, the next day there was a hearing on covert action and 12 out of 15 Senators attended and stayed throughout—and that for a covert program that is but a fraction of one percent of our total budget, and that is just one-tenth the size of the program two years

ago, and where there are virtually no controversial activities under way. Budget hearings on the House side were often attended only by the Chairman, the Ranking Minority Member, and a very small number of others, typically dropping in for a few minutes at a time.

I know that the Members can read the record of the hearing, but how many really do? The result is that enormous responsibility then falls to the staffs of the Committees. They are neither elected nor confirmed by anyone, and yet they acquire enormous influence over the structuring of issues, as well as the attitudes and votes of the members.

My concern, then, is not oversight, but the lack of attention and knowledge and time on the part of too many members of the intelligence and Appropriations Committees. This, in turn, means that in this most sensitive area of American government, anonymous staff members with little or no experience in intelligence or its use by the Executive acquire enormous power over the programs and directions of American intelligence.

To make matters worse, Congressional rules approved in the mid-1970s established time limits on Members' service on the Intelligence Committees—eight years in the Senate, six years in the House. As a result, just when an interested or concerned member begins to acquire some knowledge and understanding of our work, he or she is rotated off the Intelligence Committee—unlike most other Committees of the Congress.

So my major complaint with Congressional oversight of intelligence is that there is not enough of it—that is, by the Members of Congress themselves. Now, I am not naive. I know how the system in Congress works, and I know that the situation that I describe prevails in nearly all other areas of government as well. But, as we reduce the size of our military and contemplate major changes in the structure and size of American intelligence, I would argue strongly that these decisions are too important to be left to staff. Those in Congress who are selected for these Committees—and I am told that there is high interest in joining these Committees in both Houses—should be expected to invest the time necessary to gain an understanding of the intricate and fragile system that they seek to change. Our national security depends upon it.

The second concern that I have involves the way in which Congress is organized to deal with our budget. Again, we are on the receiving end of a larger problem identified by Congressional reformers. In past years, the Chairmen of our two Intelligence Committees have devoted enormous effort to reviewing our budget in great detail and making recommendations with respect to that budget. Until recently, the Appropriations Committees were willing to defer in considerable measure to the Intelligence Committees—and would usually see to it that the Appropriations bills paralleled the recommendations of the Intelligence Authorizing Committees. However, in the last two years or so, the appropriators have shown considerably less willingness to defer to the Intelligence Committees with the result that these two bills—the intelligence authorization bill and the separate appropriations bill—are often very different. As a result, when the appropriators tell us to do one thing and the Intelligence Committees have not acted or disagree, we are paralyzed—caught in the middle.

Let me give you an example. Last year, the Appropriations Committees approved several hundred million dollars more for intelligence than did the authorizing Intelligence Committees. We went back to all of the Committees in the spring and asked that a substantial portion of that money be approved by the Committees so that we could enhance our efforts on nonproliferation, counternarcotics and certain other high priorities. Everyone agreed with our intended use of the money, but because of minor differences and procedural squabbles among the Appropriations, Intelligence and Armed Services Committees, it

took us five months of intense effort to get these transfers approved. I don't know anyone in Congress who believes that is how the system is supposed to work.

We in intelligence also are becoming vulnerable to another common practice but one from which heretofore we have largely been protected—insistence by individual Members on funding of pet projects before they will approve our budget. At a time of significantly declining resources, this is a dangerous trend that threatens to weaken our intelligence capabilities by forcing us to spend money for programs that we do not seek and that we find wasteful.

Let me conclude by making three recommendations for strengthening Congressional oversight:

—First, Congress should end the practice of rotating Members on the Intelligence Committees. The fear in 1976 that Members of the Committees would be co-opted by the intelligence services and lose their ability to be critical has proven unfounded. At the same time, the rotation has contributed to a lack of expertise, knowledge and understanding on the part of Members of the Oversight Committees of what U.S. intelligence does, how it does it, and how it can be improved. If it is too hard to end the rotation, at a minimum the period of service should be extended substantially. As Representative Lee Hamilton said in an address at the University of Virginia on 16 December 1986, "The large turnover of Committee Membership every six years produces a loss of institutional memory {that} hinders effective oversight."

—Second, I urge the returning Members of the Intelligence Committees and the new Members to take especially seriously their responsibilities on the Oversight Committees and give them high priority. For the good of the country, they must make the time available to learn about the intelligence agencies that they oversee—how they do their work, how well they perform, the quality of the people, how they can be improved, and what intelligence capabilities this country will need in the future.

—Third, and finally, although I realize that it is a naive request, I hope that the Congressional leadership can do something about the conflict between the authorizing committees and the appropriators because the problems created by the disparity in their respective legislation is imposing a great cost on the Intelligence community both in terms of effective management and the ability to deal with high priority issues.

In the first nine months of 1992, I personally had some 120 meetings, briefings and hearings on Capitol Hill. Building on the efforts of my predecessor, Judge Webster, over several years to improve our relationship with Congress, one of the achievements of the past year about which I am the most proud was the absence for the first time of a single major problem, incident or controversy in our dealings with the Intelligence Oversight Committees.

I have just issued guidance to every employee of CIA and the Intelligence Community who may appear before Congress that stresses four principles of testifying first articulated by my predecessor, Judge William Webster: candor, completeness, correctness and consistency. I am confident that my successor will devote the same effort, in collaboration with the other leaders of the Community, to extending this period of cooperation and confidence-building between the Intelligence Community and the Congress.

I strongly support Congressional oversight of intelligence activities. I believe it is a needed check in our system. But it is also a measure of how far we have come that it is the intelligence professionals who now call for a further strengthening of Congressional oversight—that is, by the Members of Congress who accept that responsibility.

GLOSSARY

ACCM	Alternative or Compensatory Control Measure
AFIO	Association of Former Intelligence Officers
AG	Attorney General
Aman	Agaf ha-Modi'in (Israeli military intelligence)
ANC	African National Congress
BDA	Battle Damage Assessment
BfV	Bundesamt für Verfassungsschutz (German equivalent of the FBI)
BMD	Ballistic Missile Defense
BND	Bundesnachrichtendienst (German foreign intelligence service)
BSO	Black September Organization
BW	Biological Weapons
CA	Covert Action
CAS	Covert Action Staff (CIA)
CBW	Chemical/Biological Warfare
CCP	Consolidated Cryptographic Program
CDA	Congressionally Directed Action
CE	Counterespionage
CHAOS	Code name for CIA illegal domestic spying
CI	Counterintelligence
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CIG	Central Intelligence Group
CMS	Community Management Staff
CNC	Crime and Narcotics Center (CIA)

COINTELPRO	FBI Counterintelligence Program
COMINT	Communications Intelligence
Corona	Codename for first U.S. spy satellite system
COS	Chief of Station (CIA)
COSPO	Community Open Source Program Office
CPA	Covert Political Action
CPSU	Communist Party of the Soviet Union
CSI	Committee on Intelligence Services (Britain)
CT	Counterterrorism
CTC	Counterterrorism Center (CIA)
CW	Chemical Weapons
D & D	Denial and Deception
DARP	Defense Airborne Reconnaissance Program
DAS	Deputy Assistant Secretary
DBA	Dominant Battlefield Awareness
DC	Deputies Committee (NSC)
DCD	Domestic Contact Division (CIA)
DCI	Director of Central Intelligence
D/CIA	Director of Central Intelligence Agency
DDA	Deputy Director of Administration (CIA)
DDCI	Deputy Director for Central Intelligence (DDCI)
DD/CIA	Deputy Director, Central Intelligence Agency
DDO	Deputy Director for Operations (CIA)
DDP	Deputy Director for Plans (CIA)
DDS&T	Deputy Director for Science and Technology (CIA)
DEA	Drug Enforcement Administration
DGSE	Directorie Génerale de la Sécurité Extérieure (French intelligence service)
DHS	Department of Homeland Security
DI	Directorate of Intelligence (CIA)
DIA	Defense Intelligence Agency
DIA/Humint	Defense Humint Service
DINSUM	*Defense Intelligence Summary*
DNI	Director of National Intelligence
DO	Directorate of Operations
DoD	Department of Defense
DOD	Domestic Operations Division (CIA)
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Treasury
DOS	Department of State
DP	Directorate of Plans (CIA)
DST	Directoire de Surveillance Territore (France)
ECHR	European Convention of Human Rights

ELINT	Electronic Intelligence
ENIGMA	Code machine used by the Germans during World War II
EO	Executive Order
EOP	Executive Office of the President
ETF	Environmental Task Force (CIA)
FARC	Fuerzas Armadas Revolucionarias in Colombia
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FISA	Foreign Intelligence Surveillance Act (1978)
FNLA	National Front for the Liberation of Angola
FOIA	Freedom of Information Act
FRD	Foreign Resources Division (CIA)
FSB	Federal'naya Sluzba Besnopasnoti (Federal Security Service, Russia)
GAO	General Accountability Office (Congress)
GCHQ	Government Communications Headquarters (the British NSA)
GEO	Geosynchronous Orbit
GEOINT	Geospatial Intelligence
GRU	Soviet Military Intelligence
GSG	German Counterterrorism Service
HEO	High Elliptical Orbit
HPSCI	House Permanent Select Committee on Intelligence
HUAC	House Un-American Activities Committee
HUMINT	Human Intelligence (assets)
I & W	Indicators and Warning
IAEA	International Atomic Energy Agency
IAF	Israel Air Force
IC	Intelligence Community
ICS	Intelligence Community Staff
IDF	Israeli Defense Force
IG	Inspector General
IMINT	Imagery Intelligence (photographs)
INR	Bureau of Intelligence and Research (Department of State)
INTELINK	An intelligence community computer information system
INTs	Collection disciplines (IMINT, SIGINT, OSINT, HUMINT, MASINT)
IOB	Intelligence Oversight Board (White House)
ISA	Israeli Security Agency
ISC	Intelligence and Security Committee (U.K.)
ISI	Inter-Services Intelligence (Pakistani intelligence agency)
IT	Information Technology
JCAE	Joint Committee on Atomic Energy
JCS	Joint Chiefs of Staff
JIC	Joint Intelligence Committee (U.K.)

JSOC	Joint Special Operations Command
JSTARS	Joint Surveillance Target Attack Radar Systems
KGB	Soviet Secret Police
KH	Keyhole (satellite)
LTTE	Tamil Tigers of Tamil Elam
MAGIC	Allied code-breaking operations against the Japanese in the World War II
MASINT	Measurement and Signatures Intelligence
MI5	Security Service (U.K.)
MI6	Secret Intelligence Service (U.K.)
MON	Memoranda of Notification
MONGOOSE	Code name for CIA covert actions against Fidel Castro of Cuba (1961–62)
Mossad	Israeli Intelligence Service
MPLA	Popular Movement for the Liberation of Angola
NAACP	National Association for the Advancement of Colored People
NBC	Nuclear, Biological, and Chemical (Weapons)
NCS	National Clandestine Service
NCIC	National Counterintelligence Center
NCTC	National Counterterrorism Center
NED	National Endowment for Democracy
NFIB	National Foreign Intelligence Board
NFIC	National Foreign Intelligence Council
NFIP	National Foreign Intelligence Program
NGA	National Geospatial-Intelligence Agency
NGO	Nongovernmental organization
NIA	National Intelligence Authority
NIC	National Intelligence Council
NID	*National Intelligence Daily*
NIE	National Intelligence Estimate
NIO	National Intelligence Officer
NOC	Nonofficial Cover
NPIC	National Photographic Interpretation Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council (White House)
NSCID	National Security Council Intelligence Directive
NTM	National Technical Means
OB	Order of Battle
OC	Official Cover
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
ONI	Office of Naval Intelligence

OPC	Office of Policy Coordination
OSD	Office of the Secretary of Defense
OSINT	Open-Source Intelligence
OSS	Office of Strategic Services
P & E	Processing and Exploitation
PDB	*President's Daily Brief*
PFIAB	President's Foreign Intelligence Advisory Board (White House)
PFLP	Popular Front for the Liberation of Palestine
PIJ	Palestinian Islamic Jihad
PLO	Palestine Liberation Organization
PM	Paramilitary
PRO	Public Record Office (U.K.)
RADINT	Radar Intelligence
RFE	Radio Free Europe
RL	Radio Liberty
SA	Special Activities Division (DO/CIA)
SAS	Special Air Service (U.K.)
SBS	Special Boat Service (U.K.)
SDO	Support to Diplomatic Operations
SHAMROCK	Code name for illegal NSA interception of cables
SIG	Senior Interagency Group
SIGINT	Signals Intelligence
SIS	Secret Intelligence Service (U.K., also known as MI6)
SISDE	Italian Intelligence Service
SMO	Support to Military Operations
SMS	Secretary's *Morning Summary* (Department of State)
SNIE	Special National Intelligence Estimate
SO	Special Operations (CIA)
SOCOM	Special Operations Command (Department of Defense)
SOE	Special Operations Executive (U.K.)
SOG	Special Operations Group (DO/CIA)
SOVA	Office of Soviet Analysis (CIA)
SSCI	Senate Select Committee on Intelligence
SVR	Russian Foreign Intelligence Service
TECHINT	Technical Intelligence
TELINT	Telemetery Intelligence
TIARA	Tactical Intelligence and Related Activities
TPED	Tasking, Processing, Exploitation, and Dissemination
UAV	Unmanned Aerial Vehicle (drone)
ULTRA	Code name for the Allied operation that deciphered the German ENIGMA code in World War II
UN	United Nations
UNITA	National Union for the Total Independence of Angola

UNSCOM	United Nations Special Commission
USIB	United States Intelligence Board
USTR	United States Trade Representative
VCI	Viet Cong Infrastructure
VENONA	Code name for SIGINT intercepts against Soviet spying in America
VOA	Voice of America
VX	A deadly nerve agent used in chemical weapons
WMD	Weapons of mass destruction

INDEX

ABOUT THE EDITOR AND CONTRIBUTORS

EDITOR

Loch K. Johnson is Regents Professor of Public and International Affairs at the University of Georgia and author of several books and over 100 articles on U.S. intelligence and national security. His books include *The Making of International Agreements* (1984); *A Season of Inquiry* (1985); *Through the Straits of Armageddon* (1987, coedited with Paul Diehl); *Decisions of the Highest Order* (1988, coedited with Karl F. Inderfurth); *America's Secret Power* (1989); *Runoff Elections in the United States* (1993, coauthored with Charles S. Bullock III); *America as a World Power* (1995); *Secret Agencies* (1996); *Bombs, Bugs, Drugs, and Thugs* (2000); *Fateful Decisions* (2004, coedited with Karl F. Inderfurth); *Strategic Intelligence* (2004, coedited with James J. Wirtz); *Who's Watching the Spies?* (2005, coauthored with Hans Born and Ian Leigh); *American Foreign Policy* (2005, coauthored with Daniel Papp and John Endicott); and *Seven Sins of American Foreign* Policy (2007). He has served as special assistant to the chair of the Senate Select Committee on Intelligence (1975–76), staff director of the House Subcommittee on Intelligence Oversight (1977–79), and special assistant to the chair of the Aspin-Brown Commission on Intelligence (1995–96). In 1969–70, he was an American Political Science Association Congressional Fellow. He has served as secretary of the American Political Science Association and President of the International Studies Association, South. Born in New Zealand and educated at the University of California, Johnson has taught at the University of Georgia since 1979, winning its Meigs Professorship for meritorious teaching and its Owens Award for outstanding accomplishments in the field of social science research. In 2000, he led the founding of the School of Public and

International Affairs at the University of Georgia. He is the senior editor of the international journal *Intelligence and National Security*.

CONTRIBUTORS

Matthew M. Aid is Managing Director in the Washington, DC, office of Citigate Global Intelligence and Security and coeditor of *Secrets of Signals Intelligence During the Cold War and Beyond* (2001).

James E. Baker sits on the U.S. Court of Appeals for the Armed Forces. He previously served as Special Assistant to the President and Legal Adviser to the National Security Council and as Deputy Legal Adviser to the NSC. He has also served as Counsel to the President's Foreign Intelligence Advisory Board, an attorney at the Department of State, a legislative aide to Senator Daniel Patrick Moynihan, and as a Marine Corps infantry officer. He is the coauthor with Michael Reisman of *Regulating Covert Action* (Yale University Press, 1992).

David M. Barrett is Associate Professor of Political Science at Villanova University and author of *Congress and the CIA* (Kansas, 2005).

Hans Born is a senior fellow in democratic governance of the security sector at the Geneva Centre for Democratic Control of the Armed Forces (DCAF). He is an external member of the crisis management and security policy faculty of the Federal Institute of Technology and a guest lecturer on governing nuclear weapons at the UN Disarmament Fellowship Programme. He has written, co-authored, and co-edited various books on international relations and security policy, including the Inter-Parliamentary Union Handbook on *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices* (Geneva: IPU/DCAF, 2003, translated in 30 languages); *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005, translated in 10 languages); *Who is Watching the Spies? Establishing Intelligence Agency Accountability* (Dulles, VA: Potomac Publishers, 2005); *Civil-Military Relations in Europe: Learning from Crisis and Institutional Change* (London: Routledge, 2006); and *The Double Democratic Deficit: Parliamentary Accountability and the Use of Force under International Auspices* (London: Ashgate Publishers: Aldershot).

A. Denis Clift is President of the Department of Defense Joint Military Intelligence College. He was born in New York City and educated at Friends Seminary, Phillips Exeter Academy (1954), Stanford University (B.A., 1958), and the London School of Economics and Political Science (M.Sc., 1967). He began a career of public service as a naval officer in the Eisenhower and Kennedy administrations and has served in military and civilian capacities in ten administrations, including thirteen successive years in the Executive Office of the President and the White House. From 1971–76, he served on the National Security

Council staff. From 1974–76, he was head of President Ford's National Security Council staff for the Soviet Union and Eastern and Western Europe. From 1977–81, he was Assistant for National Security Affairs to the Vice President. From 1991–94, he was Chief of Staff, Defense Intelligence Agency. From 1963–66, he was the editor of the U.S. Naval Institute *Proceedings*. His published fiction and nonfiction include the novel *A Death in Geneva* (Ballantine Books, Random House), *Our World in Antarctica* (Rand McNally), *With Presidents to the Summit* (George Mason University Press), and *Clift Notes: Intelligence and the Nation's Security* (JMIC Writing Center Press).

William J. Daugherty holds a doctorate in government from the Claremont Graduate School and is Associate Professor of government at Armstrong Atlantic State University in Savannah, Georgia. A retired senior officer in the CIA, he is also the author of *In the Shadow of the Ayatollah: A CIA Hostage in Iran* (Annapolis, 2001) and *Executive Secrets: Covert Action and the Presidency* (Kentucky, 2004).

Jack Davis served in the CIA from 1956 to 1990 as analyst, manager, and teacher of analysts. He now is an independent contractor with the Agency, specializing in analytic methodology. He is a frequent contributor to the journal *Studies in Intelligence*.

Stuart Farson is Lecturer, Political Science Department, Simon Fraser University, Vancouver/Surrey, Canada. He is a former Secretary-Treasurer of the Canadian Association for Security and Intelligence Studies, and served as Director of Research for the Special Committee of the House Commons (Canada) on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act. He has numerous articles on security, intelligence, and policing issues and is the coeditor of *Security and Intelligence in a Changing World* (with David Stafford and Wesley K. Wark, Cass, 1991).

Timothy Gibbs is a final-year doctoral student in history at Robinson College, Cambridge University, and a member of the Cambridge University Intelligence Seminar. He is also a former Visiting Scholar at the University of Georgia. His doctoral dissertation, titled *British and American Intelligence and the Atom Spies*, was submitted in the summer of 2006 and was supervised by Professor Christopher Andrew.

Peter Gill is Reader in Politics and Security, Liverpool John Moores University, Liverpool, United Kingdom. He is coauthor of *Introduction to Politics* (1988, 2nd ed.) and *Intelligence in an Insecure World* (2006). He is currently researching the control and oversight of domestic security in intelligence agencies.

Harold M. Greenberg graduated with a B.A. in history from Yale University in 2005. At Yale, he participated in the Studies in Grand Strategy program, and he has recently published research on CIA covert action in the 1950s. He now works as a legislative aide in the U.S. House of Representatives.

Daniel S. Gressang IV is Professor at the Joint Military Intelligence College (JMIC) in Washington, DC, and serves concurrently as the National Security Agency/National Cryptologic School of Liaison to JMIC. He has researched, written, and lectured extensively on terrorism and counterinsurgency. His research focuses primarily on the application of complex adaptive systems perspectives to understanding the dynamics of terror and other forms of unconventional warfare. In 2004, he was designated Intelligence Community Officer by the Director of Central Intelligence.

Glenn Hastedt received his doctorate in political science from Indiana University. Until recently he was Professor and Chair of the Political Science Department at James Madison University. He is now chair of the Justice Studies Department there. Among his publications is *American Foreign Policy: Past, Present, Future*, 6th ed. (Prentice Hall).

John Hollister Hedley, during more than thirty years at CIA, edited the *President's Daily Brief*, briefed the *PDB* at the White House, served as Managing Editor of the *National Intelligence Daily*, and was Chairman of the CIA's Publications Review Board. Now retired, Hedley has taught intelligence at Georgetown University and serves as a consultant to the National Intelligence Council and the Center for the Study of Intelligence.

Michael Herman served from 1952 to 1987 in Britain's Government Communications Headquarters, with secondments to the Cabinet Office and the Ministry of Defence. Since retirement he has written extensively on intelligence matters, with official clearance. He has had academic affiliations with Nuffield and St. Antony's Colleges in Oxford and is Founder Director of the Oxford Intelligence Group and Honorary Departmental Fellow at Aberystwyth University. In 2005 he received the degree of Honorary D.Litt from Nottingham University. He is a leading British intelligence scholar and author of *Intelligence Power in Peace and War* (Cambridge, 2001).

Frederick P. Hitz is Lecturer (Diplomat in Residence) in Public and International Affairs, Woodrow Wilson School, Princeton University.

Max M. Holland is the author of *The Kennedy Assassination Tapes* (Knopf, 2004).

Arthur S. Hulnick is Associate Professor of International Relations at Boston University. He is a veteran of thirty-five years of intelligence service, including seven years in Air Force Intelligence and twenty-eight years in the CIA. He is author of *Fixing the Spy Machine* (Praeger, 1999) and *Keeping Us Safe* (Praeger, 2004).

Rhodri Jeffreys-Jones is Professor of American History at the University of Edinburgh. The author of several books on intelligence history, he is currently completing a study of the FBI.

Ephraim Kahana is Professor of Political Science and faculty member in the Western Galilee College, Acre, Israel. He teaches courses on international relations, national security and intelligence, and foreign policy in the National Security Program in the University of Haifa. Kahana has written numerous papers on intelligence and foreign policy. His most recent book is the *Historical Dictionary of Israeli Intelligence* (2006).

Patrick Radden Keefe is a graduate of the School of Law at Yale University and is presently a Fellow with the Century Foundation in New York City. He is the author of *Chatter: Uncovering the Echelon Surveillance Network and the Secret World of Global Eavesdropping* (Random House, 2006), and has published essays in *The New York Review of Books*, *The New York Times Magazine*, the *New York Times*, the *Boston Globe*, the *Yale Journal of International Law*, *Legal Affairs*, *Slate*, and *Wired*. He has been a Marshall Scholar and a 2003 fellow at the Dorothy and Lewis B. Cullman Center for Scholars and Writers at the New York Public Library.

Jennifer D. Kibbe is Assistant Professor of Government at Franklin and Marshall College. Between 2002 and 2004, she was a postdoctoral fellow at the Brookings Institution. Her research interests include U.S. foreign policy, intelligence and covert action, presidential decision making, and political psychology. She has published work on U.S. policy in Iraq and the Middle East, and the military's involvement in covert actions.

Katharina von Knop is a doctoral candidate in Political Science at Leopold-Franzens University in Innsbruck, Austria, specializing in counter- and antiterrorism, and coeditor with Heinrich Neisser and Martin van Creveld of *Countering Modern Terrorism: History, Current Issues, and Future Threats* (2005).

Lawrence J. Lamanna is a doctoral candidate in the School of Public and International Affairs at the University of Georgia. He holds an M.A. from Yale University and a B.A. from the University of Notre Dame.

Ian Leigh is Professor of Law and Codirector of the Human Rights Centre at the University of Durham. He lives in Durham, England.

Kristin M. Lord is Associate Dean at George Washington University's Elliott School of International Affairs. In 2005–2006, she was a Council on Foreign Relations International Affairs Fellow and Special Adviser to the Under Secretary of State for Democracy and Global Affairs. Lord is the author of *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security Democracy or Peace* (SUNY Press, 2006); coeditor, with Bernard I. Finel, of *Power and Conflict in the Age of Transparency* (Palgrave Macmillan, 2000); and the author of numerous book chapters, articles, and papers on international politics and security. Lord received her doctorate in government from Georgetown University.

Minh A. Luong is Assistant Director of International Security Studies at Yale University, where he teaches in the Department of History. He also serves as adjunct Assistant Professor of Public Policy at the Taubman Center at Brown University.

Cynthia M. Nolan earned a doctorate at American University in the School of International Service, researching intelligence oversight. She is a former officer in the Directorate of Operations in the CIA and has published in the *International Journal of Intelligence and Counterintelligence*.

Kevin A. O'Brien is a former research associate with the Canadian Institute of Strategic Studies and is currently a senior analyst for RAND Europe.

Mark Phythian is Professor of International Security and Director of the History and Governance Research Institute at the University of Wolverhampton, United Kingdom. He is the author of *Intelligence in an Insecure World* (2006, with Peter Gill), *The Politics of British Arms Sales Since 1964* (2000), and *Arming Iraq* (1997), as well as numerous journal articles on intelligence and security issues.

Harry Howe Ransom is Professor Emeritus of Political Science at Vanderbilt University. He has a B.A. from Vanderbilt and an M.A. and Ph.D. from Princeton University. He was a Congressional Fellow of the American Political Science Association and a Fellow of the Woodrow Wilson International Center for Scholars. He taught at Princeton, Vassar College, Michigan State University, Harvard University, and the University of Leeds. His books include *Central Intelligence and National Security* (1958), *Can American Democracy Survive Cold War?* (1963), and *The Intelligence Establishment* (1970).

Jeffrey T. Richelson is Senior Fellow with the National Security Archive in Washington, DC, and author of *The Wizards of Langley*, *The U.S. Intelligence Community*, *A Century of Spies*, and *America's Eyes in Space*, as well as numerous articles on intelligence activities. He received his doctorate in political science from the University of Rochester and has taught at the University of Texas, Austin, and the American University, Washington, DC. He lives in Los Angeles.

Jerel A. Rosati is Professor of Political Science and International Studies at the University of South Carolina since 1982. His area of specialization is the theory and practice of foreign policy, focusing on the U.S. policy-making process, decision-making theory, and the political psychological study of human cognition. He is the author and editor of five books and over forty articles and chapters. He has received numerous outstanding teaching awards. He has been Visiting Professor at Somalia National University in Mogadishu and Visiting Scholar at China's Foreign Affairs College in Beijing. He also has been a Research Associate in the Foreign Affairs and National Defense Division of the Library of Congress's Congressional Research Service, President of the International

Studies Association's Foreign Policy Analysis Section, and President of the Southern region of the International Studies Association.

Richard L. Russell is Professor of national security studies at the National Defense University. He is also an adjunct associate professor in the Security Studies Program and research associate in the Institute for the Study of Diplomacy at Georgetown University. He previously served as a CIA political-military analyst. Russell is the author of *Weapons Proliferation and War in the Greater Middle East: Strategic Contest* (2005).

Frederick A. O. Schwarz Jr. received an A.B. from Harvard University and J.D. from Harvard Law School, where he was an editor of the *Law Review*. After a year's clerkship with Hon. J. Edward Lumbard, U.S. Court of Appeals for the Second Circuit, he worked one year for the Nigerian government as Assistant Commissioner for Law Revision under a Ford Foundation grant. He joined the New York City law firm of Cravath, Swaine and Moore in 1963 and was elected a partner in 1969. From 1975 through mid-1976, he served as Chief Counsel to the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the Church Committee); from 1982–89, he served as Corporation Counsel and head of the Law Department of the City of New York. In 1989, he chaired the New York City Charter Revision Commission.

James M. Scott is Professor and Chair of the Department of Political Science at Oklahoma State University. His areas of specialization include foreign policy analysis and international relations, with particular emphasis on U.S. foreign policy making and the domestic sources of foreign policy. He is author or editor of four books, over forty articles, book chapters, review essays, and other publications. He has been President of the Foreign Policy Analysis section and President of the Midwest region of the International Studies Association, where he has also served as conference organizer for both sections and has been a two-time winner of the Klingberg Award for Outstanding Faculty Paper at the ISA Midwest Annual Meeting. Since 1996, he has received over two dozen awards from students and peers for his outstanding teaching and research, including his institution's highest awards for scholarship in 2000 and 2001. Since 2005, he has been Director of the Democracy and World Politics Summer Research Program, a National Science Foundation Research Experience for Undergraduates.

Len Scott is Professor of International Politics at the University of Wales, Aberystwyth, where he is Director of the Centre for Intelligence and International Security Studies. Among his recent publications are *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows* (2004, coedited with Peter Jackson) and *Planning Armageddon: Britain, the United States and the Command of Nuclear Forces, 1943–1964* (2000, coedited with Stephen Twigge).

Katherine A. S. Sibley is Professor and Chair of the History Department at St. Joseph's University. She is currently working on a biography of Florence Kling

Harding, titled *America's First Feminist First Lady*. Sibley's work will revise the typical portrait of Mrs. Harding as manipulative, unhappy wife, casting new light on her public and private life. In 2004, Sibley published *Red Spies in America: Stolen Secrets and the Dawn of the Cold War* with the University Press of Kansas. She is also the author of *The Cold War* (1998) and *Loans and Legitimacy: The Evolution of Soviet-American Relations, 1919–1933* (1996). Her work has appeared in journals including *American Communist History*, *Peace and Change*, and *Diplomatic History*, and she also serves as book review editor for *Intelligence and National Security*. She is a three-term Commonwealth Speaker for the Pennsylvania Humanities Council.

Jennifer Sims is Director of Intelligence Studies and Visiting Professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service. She also consults for the U.S. government and private sector on homeland security and intelligence related matters. Prior to this, Sims was Research Professor at Johns Hopkins University's Nitze School of Advanced International Studies in Washington, DC (Fall 2001–Summer 2003). She has served as defense and foreign policy adviser to Senator John Danforth (1990–94), a professional staff member of the Senate Select Committee on Intelligence (1991–94), Deputy Assistant Secretary of State for Intelligence Coordination (1994–98), and as the Department of State's first Coordinator for Intelligence Resources and Planning in the office of the Under Secretary for Management. In 1998 Sims was awarded the U.S. Intelligence Community's Distinguished Service Medal. She received her B.A. degree from Oberlin College and her M.A. and Ph.D. in national security studies from Johns Hopkins University in 1978 and 1985, respectively. She is the author of a number of books and articles on intelligence and arms control. The most recent of these include "Foreign Intelligence Liaison: Devils, Deals and Details," *International Journal of Intelligence and Counterintelligence Affairs* (Summer 2006); *Transforming US Intelligence,* coedited with Burton Gerber (Georgetown University Press, 2005); "Transforming U.S. Espionage: A Contrarian's Approach," *Georgetown Journal of International Affairs* (Winter/Spring 2005); "Domestic Factors in Arms Control: The U.S. Case," in Jeffrey A Larson (ed.), *Arms Control: Cooperative Security in a Changing Environment* (Lynne Rienner, 2002); "What Is Intelligence? Information for Decision-Makers," in Roy Godson, Ernest R. May, and Gary Schmitt, *U.S. Intelligence at the Crossroads* (Brassey's, 1995); "The Cambridge Approach Reconsidered," *Daedalus* 120 (Winter 1991); and *Icarus Restrained: An Intellectual History of American Arms Control* (Westview Press, 1990).

Robert David Steele is CEO of OSS.Net, an international open source intelligence provider. As the son of an oilman, a Marine Corps infantry officer, and a clandestine intelligence case officer for the CIA, he has spent over twenty years abroad in Asia and Central and South America. As a civilian intelligence officer he spent three back-to-back tours overseas, including one tour as one of the first officers assigned full-time to terrorism, and three headquarters tours in offensive

counterintelligence, advanced information technology, and satellite program management. He resigned from the CIA in 1988 to be the senior civilian founder of the Marine Corps Intelligence Command. He resigned from the Marines in 1993. He is the author of three works on intelligence, as well as the editor of a book on peacekeeping intelligence. He has earned graduate degrees in international relations and public administration, is a graduate of the Naval War College, and has a certificate in Intelligence Policy. He is also a graduate of the Marine Corps Command and Staff Course and of the CIA's Mid-Career Course 101.

John D. Stempel is Senior Professor of International Relations at the University of Kentucky's Patterson School of Diplomacy and International Commerce, where he was Associate Director (1988–93) and Director (1993–2003). He came to the University of Kentucky following a 24-year career in the U.S. Foreign Service. There he focused on political and economic affairs, with overseas assignments in Africa (Guinea, Burundi, Zambia), Iran, and India, concluding with three years as U.S. Consul General in Madras. His Middle East service (1975–79) in Tehran provided the material for his book *Inside the Iranian Revolution*. His subsequent academic writings have focused on religion and diplomacy, intelligence and diplomacy, and American views of negotiation. His Washington assignments featured duty for both the State and Defense Departments, including a two-year tour as Director of the State Department's Crisis Center. He has taught at George Washington and American Universities, plus two years as Diplomat in Residence at the U.S. Naval Academy, Annapolis. Stemple is a member of the New York Council on Foreign Relations and is listed in *Who's Who in the World* and *Who's Who in America*. He holds an A.B. degree from Princeton University and M.A. and Ph.D. degrees from the University of California at Berkeley.

Stan A. Taylor is an Emeritus Professor of Political Science at Brigham Young University in Provo, Utah. He has taught in England, Wales, and New Zealand and in 2006 was a visiting professor at the University of Otago in Dunedin, New Zealand. He is founder of the David M. Kennedy Center for International Studies at Brigham Young University. He writes frequently on intelligence, national security, and U.S. foreign policy.

Athan Theoharis is Professor of History at Marquette University whose research has focused on government secrecy, Cold War politics, and the history of the FBI. He is the author, coauthor, and editor of eighteen books, including *The FBI and American Democracy* (2004), *Chasing Spies* (2002), *A Culture of Secrecy* (1998), and *The FBI: A Comprehensive Reference Guide* (1998). He has received numerous awards, including the American Bar Association's Gavel Award and selection as a fellow by the Wisconsin Academy of Arts, Sciences, and Letters.

Gregory F. Treverton is senior analyst at the RAND Corporation. Earlier, he directed RAND's Intelligence Policy Center and its International Security and Defense Policy Center, and he is Associate Dean of the Pardee RAND Graduate School. His recent work has examined at terrorism, intelligence, and law

enforcement, with a special interest in new forms of public-private partnership. He has served in government for the first Senate Select Committee on Intelligence, handling Europe for the National Security Council, and most recently as vice chair of the National Intelligence Council, overseeing the writing of America's National Intelligence Estimates. He holds an A.B. *summa cum laude* from Princeton University, a master's in public policy, and Ph.D. in economics and politics from Harvard University. His latest books are *Reshaping National Intelligence for an Age of Information* (Cambridge University Press, 2001), and *New Challenges, New Tools for Defense Decisionmaking* (edited, RAND, 2003).

Michael A. Turner is a political scientist who has taught international relations and national security matters in San Diego, California, for the past twelve years. Before that, he spent over fifteen years in various positions within the CIA. Turner is the author of *Why Secret Intelligence Fails* (2005; 2006) and the *Historical Dictionary of United States Intelligence* (2006).

Michael Warner serves as Historian for the Office of the Director of National Intelligence.

Nigel West is a military historian specializing in security and intelligence topics. He is the European editor of the *World Intelligence Review* and is on the faculty at the Center for Counterintelligence and Security Studies in Washington, DC. He is the author of more than two dozen works of nonfiction and recently edited *Guy Liddell Diaries*.

Reg Whitaker is Distinguished Research Professor Emeritus, York University, and Adjunct Professor of Political Science, University of Victoria, Canada. He has written extensively on Canadian and international security and intelligence issues.

James J. Wirtz is Professor in the Department of National Security Affairs at the Naval Postgraduate School, Monterey, California. He is Section Chair of the Intelligence Studies Section of the International Studies Association and President of the International Security and Arms Control Section of the American Political Science Association. Wirtz is the series editor for *Initiatives in Strategic Studies: Issues and Policies*, published by Palgrave Macmillan.

Amy B. Zegart is Associate Professor of Public Policy at the University of California, Los Angeles. A specialist on national and homeland security, she has served on the National Security Council staff, as a foreign policy advisor to the Bush-Cheney 2000 presidential campaign, and as a consultant to California state and local homeland security agencies. She has published articles in leading academic journals, including *International Security* and *Political Science Quarterly*, and is the author of *Flawed by Design: The Origins of the CIA, JCS, and NSC* (Stanford, 1999). She received her Ph.D. in political science from Stanford, where she studied under Condoleezza Rice, and an A.B. in East Asian Studies from Harvard University.