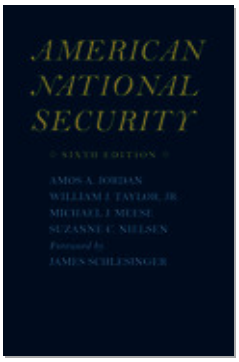
# American National Security

Jordan, Amos A., Taylor, Jr., William J., Meese, Michael J., Nielsen, Suzanne C., Schlesinger, James




Published by Johns Hopkins University Press

# 7

# Intelligence and National Security

The Framers of the Constitution foresaw, in Alexander Hamilton's words, that "accurate and comprehensive knowledge of foreign politics" would inevitably be required in the management of America's external relations.[1] Intelligence, managed prudently, would be a useful and indeed necessary capability for the infant republic.[2] More than two hundred years later, national security policy makers in the more mature American republic still recognize their reliance on, and indebtedness to, accurate information about the external world. When intelligence fails, as it did on the issue of whether Saddam Hussein's regime had weapons of mass destruction (WMDs) prior to the U.S.-led invasion of Iraq in 2003, the consequences for U.S. policy can be significant.

## What Is Intelligence?

The concept of intelligence is often confused with information.[3] Although information is anything that can be known, *intelligence* is a subset that includes information selected or tailored to respond to policy requirements or needs: "Intelligence refers to information relevant to a government's formulation and implementation of policy to further its national security interests and to deal with threats from actual or potential adversaries."[4] Although many associate the term strictly with military information, intelligence for national security is more than a description and analysis of armed capabilities. It also can include political, economic, social, cultural, and technological aspects of an adversary.[5] One way of categorizing intelligence is to refer to the time horizon in which intelligence is expected to be used.[6] Strategic intelligence examines issues with long-term implications, such as political and economic trends over time. Tactical intelligence, on the other hand, responds to immediate,

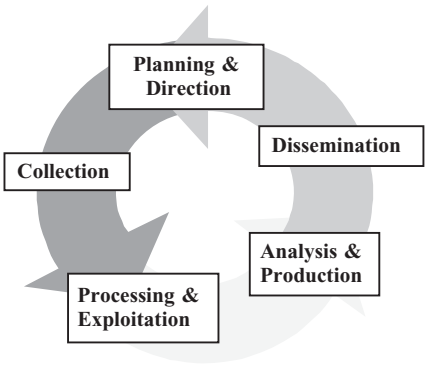
pressing concerns and is intended to inform near-term decisions.[7] Some of the threats now present in the external environment, such as new nuclear weapons states or terrorist networks, have resulted in increased concern over effectiveness at gathering and using extremely time-sensitive intelligence. As a recent study summarizes, "the first priority should always be to get there before the bomb goes off."[8]

Intelligence professionals exist to support decision makers. The role that members of the intelligence community play in policy making is ideally that of "seasoned and experienced advisors," who add expert analysis to collected information.[9] Intelligence professionals attempt to envision possible or likely futures by analyzing and synthesizing current data and provide decision makers with background projections against which to measure policy alternatives. They may also develop policy options for policy makers and provide an analytical basis for choice among the options. An example of this direct policy use is furnished by Secretary of State Henry Kissinger's specific request to the CIA, shortly after the 1973 Middle East War, "to examine all aspects of possible Sinai withdrawal lines on the basis of political, military, geographic, and ethnic considerations. Eight alternative lines were prepared for the Sinai, a number of which Secretary Kissinger used in mediating the negotiations between Egypt and Israel."[10] Although the best intelligence cannot guarantee sound policy, policy made with inadequate intelligence support can succeed only by accident.

## The Intelligence Production Process

Intelligence is divided into a five-part cycle: planning and direction; collection; processing and exploitation; analysis and production; and dissemination. As with all theoretical constructs, the intelligence cycle model is not perfect in describing reality.[11] Although an actual intelligence process may involve more complex and dynamic interactions, the conceptual clarity of the intelligence cycle is of great utility in structuring thinking about core intelligence functions. The five stages of the intelligence cycle are depicted in Figure 7.1 and will be discussed in turn below.

**FIG. 7.1** The Intelligence Cycle




*Source:* Adapted from www.intelligence.gov/2-business.shtml

**Planning and Direction.** Consumers (policy makers and their advisers) take an active role in the *planning and direction* phase, which in turn influences the entire intelligence process.[12] The planning stage of the cycle begins with the determination of the consumers' specific information needs or a reaffirmation of continuing interests. Intelligence managers review consumer requests, and, if ongoing efforts or existing databases are unable to satisfy them, these requests are approved as new intelligence requirements. These requirements are then tasked to agencies with the requisite operational capabilities. Requirements developed through this process may be long term and require continuous attention, or they may generate a discrete project.

Problems in the planning stage stem from two areas: first, the development of national security policy; and second, the management of the intelligence community to inform that policy.[13] On the first issue, national security policy may not be sufficiently clear or specific with regard to content or priorities to provide adequate guidance to intelligence planners. On the second issue, inadequate management can cause agencies within the intelligence community to work at cross purposes with one another, making it difficult to create a timely, consolidated intelligence picture.[14]

**Collection.** Once requirements have been established, the second stage of the intelligence cycle is *collection*. There are six basic methods of intelligence collection: open-source intelligence, human intelligence, signals intelligence, imagery intelligence, measurement and signature intelligence, and geospatial intelligence.[15] Taken together, they can be complementary in facilitating the cross-checking of data. Each has unique capabilities that can offset limitations of the others.

*Open-Source Intelligence.* Open-source intelligence (OSINT) is derived from print and broadcast news; academic studies; popular literature; the Internet; and other freely available, "open-source" media. With advances in information technology, the Internet and other resources create easy access to an "explosion of information," shifting the challenge away from being one of information scarcity to that of distilling relevant material from information overabundance.[16] The major collectors of OSINT in the intelligence community are the Foreign Broadcast Information Service and the National Air and Space Intelligence Center.[17]

A very large part of the intelligence on most issues comes from open sources. Due to the threat of attack from international terrorist networks, open-source information is especially important. The Internet and public media are often used by terrorists to pass private messages or incite mass politics.[18] Open-source information can be essential in understanding the ideology and strategic plans of terrorist groups, such as al-Qa'ida.[19]

*Human Intelligence.* Human intelligence (HUMINT) is information collected from a human source via overt or covert means. Examples of government collectors

include attachés and intelligence agents.[20] Sources originating from the adversary's side can come in two forms: friendly (walk-in or refugee) or hostile (detainees or prisoners of war). Though crucial, human intelligence receives only a small fraction of all the resources devoted to intelligence collection. Technological collection systems (such as imagery satellites) are more expensive and also extremely capable against certain types of intelligence problems. However, human intelligence may be the best—and, on occasion, the only—method for gaining reliable information on the intentions of an adversary's leaders. As the intelligence community increasingly focuses on nonstate actors, HUMINT will become even more important in gaining understanding of aspects of the threat.[21]

The production of quality HUMINT is accompanied by many challenges. First, running HUMINT operations can be difficult. Obstacles range from language barriers to the difficulties associated with persuading people to do things that may be against their own best interests. Second, information garnered from human beings will only be as reliable and insightful as the sources themselves. Objectivity and accuracy may be hard to judge. Third, great patience—sometimes over the course of years—may be required for the cultivation of important sources. Finally, HUMINT operations cannot be done remotely. Those involved may face danger and are also susceptible to adversary counterintelligence efforts.[22] The importance of human intelligence against such national security challenges as terrorism increases the potential benefits that can be derived from effective collaboration with foreign intelligence services.

*Signals Intelligence.* Signals intelligence (SIGINT) is subdivided into three areas: communications intelligence (COMINT); electronic intelligence (ELINT), which is primarily the interception of radar signals; and foreign instrumentation signals intelligence (FISINT), which is the interception of instrumentation signals, such as radio command signals.[23] Depending on the target's characteristics, a communications intercept analyst may gain access to only the *externals* (such data as activity time, frequency, location, or similar characteristics). In some cases, however, the analyst will also gain access to the *internals* (the content) of intercepted communications. The interception of noncommunications emitters can also provide analysts with critical information about threat activity or intentions.[24]

Although SIGINT is a tremendously productive collection method, it is also expensive in terms of money and human resources. The sheer volume of information gathered is staggering. In addition, with the advance of information technology, new denial and deception techniques to avoid interception are constantly being created and used. Problems also stem from access and legality issues. A final concern is that, as with all collection methods, the use of actionable intelligence from SIGINT may result in a compromise of the collection method and source.[25]

*Imagery Intelligence.* Imagery intelligence (IMINT) includes representations of objects reproduced electronically or by optical means on film, electronic display

devices, or other media. Imagery collection efforts use photography and related imagery-producing techniques from *nonair breathers* (space-based satellites with surveillance equipment) and *air breathers* (manned or unmanned aircraft with surveillance equipment). Types of IMINT products include electro-optical, multispectral, infrared, and radar imagery.[26]

Imagery intelligence often enables the study of areas that would otherwise be inaccessible. Although expensive, unmanned aerial collection platforms give real-time intelligence while reducing the risk to human life. Imagery is also graphic and compelling intelligence; with the right interpretation, it is easy to understand. Downsides to IMINT include the fact that satellite orbits are predictable, thus allowing adversaries to avoid detection. Air breathers are less predictable and can be diverted instantly to a target, but they may have limited dwell-time capabilities.[27] Despite remarkable advances in technology, it is important to keep in mind that reconnaissance and surveillance systems cannot see everything. The United States was reminded of this as it sought to find Iraqi SCUD missiles in the desert during the 1991 war in the Persian Gulf, and again a decade later as it looked for WMDs in Iraq before and after the 2003 U.S.-led invasion.

*Measurement and Signature Intelligence.* Professionals producing measurement and signature intelligence (MASINT) employ a broad group of techniques relating to optical, radio frequency, thermal, acoustic, seismic, and material characteristics of targets. Examples of MASINT include intelligence garnered from the noise of passing vehicles or the chemical composition of air and water samples.[28]

*Geospatial Intelligence.* A newer method, geospatial intelligence (GEOINT), is the analysis and visual representation of security-related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information.[29]

**Processing and Exploitation.** The third phase of the intelligence cycle takes collected information and makes it relevant. Considerable resources are devoted to *processing and exploitation*, or the "synthesis of raw data into a form usable by the intelligence analyst or other consumers," and also to the secure telecommunications networks used to store it.[30] Without this stage, data collected is just information without significance. For example, reels of intercepted communications are of no utility until exploited by trained analysts: "No one has any use for intelligence that is gathered and not processed—that is, teased out for the most relevant and timely pieces of information."[31] Intelligence processing can involve "exploiting imagery; decoding messages and translating broadcasts; reducing telemetry to meaningful measures; preparing information for computer processing; storage and retrieval; [and] placing human-source reports into a form and context to make them more comprehensible."[32] These processes are carried out across the entire intelligence community.[33]

**Analysis and Production.** In the fourth stage of the intelligence cycle, collected intelligence that has been exploited and processed is further collated, assessed, related, integrated, and made understandable. Intelligence analysts are ideally experts in all aspects of their targets—including the language and culture—and also adept at integrating volumes of data produced by a variety of collection methods into a comprehensive, coherent, and succinct portrayal.[34] For even the best analysts, fragmentary and uncertain information makes prediction problematic. Instead of predicting the future, the analyst spots and highlights trends, assigns probabilities to various outcomes, and illuminates choices available to policy makers. This stage is critical to the effectiveness of the overall intelligence effort. Because a policy maker can only read a portion of available intelligence, the analytical quality and brevity of intelligence reports clearly affect the quality of national security decision making.

One of the more intractable problems of the intelligence process is bias. The analyst must act as a funnel, condensing and interpreting large amounts of raw information to create a succinct intelligence report or briefing. During this process, the analyst's personal knowledge and experience will affect the final product. The problem of bias can manifest itself in several ways. A first problem is that of *projection* or *mirror-imaging*, in which an analyst attributes personal value systems and thought processes to his or her analytical subject. This can result in flawed analyses, because the subject may not operate according to the analyst's standard of logic or rationality. Bias may also stem from the conscious or unconscious incorporation of personal or organizational interests into one's assessments. An example of the latter could be the inflation of military threat estimates by an analyst to support budget interests. Intelligence analysts could also become reluctant to challenge their agency's view or party line.

In addition to problems with mirror-imaging or parochial behavior, three additional sources of bias are status quo bias, wishful thinking, and premature closure. The *status quo bias* causes an analyst to expect continuity in a target. *Wishful thinking* relates to a tendency of an analyst to avoid uncomfortable conclusions. Finally, *premature closure* relates to a situation in which an analyst makes an early judgment and then is resistant to future contradictory information.[35] Although efficiency is a legitimate concern, some competition and duplication within the intelligence community can provide a healthy cross-check against blind spots and biases.

When dealing with vast amounts of raw data, analysts risk oversimplifying reality and failing to alert the consumer to the dangers within ambiguities. As mentioned in the context of OSINT, an excess of information can sometimes be as much of a challenge as a lack of information: "Technological advances have . . . produced a 'paradox of plenty.' Plenty of information leads to scarcity—of attention."[36] Constraints in this phase stem from both funding and time. Intelligence managers must accept risk by deciding where to focus their limited resources and do their best to ensure that uncertainties are accurately conveyed.[37]

**Dissemination and Feedback.** In the final stage, intelligence products—usually written reports or briefings—are disseminated to other interested agencies

and to consumers, such as law enforcement agencies, the military, or policy makers, who can act on them. As with all the stages in the intelligence cycle, dissemination is also marked with challenges. The product must go to all who need it—at times, foreign as well as domestic consumers—and be timely enough to be helpful. At times, the classification of intelligence can make it unusable by certain consumers.[38] This challenge can be particularly acute for such issues as counterterrorism that require high levels of interagency coordination.

Because of the sensitivity of intelligence sources and methods, as well as the content of intelligence reporting, the traditional intelligence community approach to dissemination has been based on the concept of *need to know*. In other words, only other agencies and policy makers with a specific need for highly classified information would gain access to it. In reaction to the complexity of the current threat environment and the need for extensive cooperation within and among government agencies within the U.S. federal system, there has been a recent shift in emphasis to *responsibility to provide*—that is, finding a way to disseminate intelligence to all who may have a need for it.[39] Though this philosophy may improve dissemination, some constraints relating to procedures and levels of classification will persist.

If the original information needs are not satisfied, or if new questions emerge, consumers may restart the intelligence cycle by generating additional intelligence requirements. This feedback loop drives future intelligence operations. The process is a continuous one, with many requirements in various phases of the cycle at all times. However, the production of intelligence does not always follow this model. Consumers seldom take the time to articulate even their major continuing interests with a precision sufficient to drive the cycle. As a result, intelligence managers frequently generate information needs and requirements, providing consumers with intelligence they need but cannot or do not specifically request.

## The Importance of the Policy Maker in the Intelligence Production Process

As noted earlier in this chapter, the reason for the intelligence community's existence is to meet the needs of the makers and implementers of national security policy. Accordingly, an effective relationship between intelligence professionals and policy makers is important. However, in practice, the role of the intelligence community can fluctuate with each new administration and sometimes even by issue area.[40]

Policy makers can increase the quality and relevance of intelligence by clearly stating priorities and initiating requests. Nevertheless, experienced intelligence officials agree that one of the most striking and persistent deficiencies affecting intelligence production is the "inadequacy of guidance by policy-makers as to their needs."[41] When the prioritization of threats is not clear, the intelligence community is left to "play daily triage" in response to pressing national security issues.[42] Unfortunately, "this is too often a hit-or-miss proposition, because it depends on the inclination of analysts who are dealing with other pressing problems."[43]

Policy makers may also be more effective consumers of intelligence if they are aware of its limitations as well as its capabilities. For a variety of reasons, including limited collection resources, time, limited expertise, and adversary efforts at deception and denial, there is no way to know everything. As one intelligence official states, "The point to keep in mind is that perfection in intelligence is not achievable. By its very nature it is an imperfect process."[44] Intelligence can "identify current developments and trends that will shape the future and affect U.S. interests" and give policy makers "a much better understanding of the situation they face."[45] However, at the time of decision, there will still be room for judgment, and even good intelligence and accurate predictions cannot prevent bad policy choices.

A key challenge for analysts is to meet policymaker needs while still adequately conveying uncertainties.[46] Policy makers can become dismissive of intelligence that is either too imprecise or too uncertain. For example, General Norman Schwarzkopf noted in his report to Congress after the 1991 Persian Gulf War that intelligence reports were so "caveated, footnoted, and watered down that we [the forces] would still be sitting over there if we were dependent on that analysis."[47] Though analyses that are more forceful and unqualified are more likely to be influential, intelligence professionals must remain accurate and not overstate their cases.

In addition to playing positive roles in the intelligence process, policy makers can also play negative roles if their involvement results in the politicization of intelligence. Described as "an act of intellectual corruption," politicization can stem from both the consumer and the producer.[48] *Downward politicization* occurs when the policy maker influences analytical conclusions by incentivizing desired conclusions or, more subtly, by being intolerant of unwanted information or analyses.[49] Analysts who carve out or shape information to please a superior or to fit a specific desired outcome engage in *upward politicization*. Many critics, in and out of government, have charged that senior civilians in the Department of Defense (DoD) were guilty of politicizing intelligence leading up to the 2003 U.S.-led invasion of Iraq. Politicization inevitably reduces the quality of the intelligence product.

A critical issue in the environment following the terrorist attacks of September 11, 2001, has been the need for *actionable* intelligence, particularly relating to future terrorist threats. Information is evaluated according to a number of criteria: (1) specificity as to time, location, manner, perpetrator; (2) credibility of sources; (3) corroboration of information by multiple sources; and (4) potential severity of consequences. Analysts use these criteria in evaluating whether information needs to go to key decision makers, and policy makers use them to decide whether they have sufficient basis to take action.

## The Policy Implementation or Covert Action Role of Intelligence

In addition to producing intelligence, portions of the intelligence community also have the capability to act more directly as instruments of foreign policy through

covert action. *Covert action* is activity performed by the U.S. government to influence political, economic, or military conditions abroad, where it is intended that the role of the U.S. government not be apparent or acknowledged publicly.[50] Especially during the Cold War era, American leaders conceived of and used the intelligence agencies as means of affecting or influencing events abroad in accordance with U.S. foreign policy goals. Among these implementing actions have been such activities as subsidizing foreign newspapers and political parties, arming guerrilla forces, and supporting foreign military organizations or operations logistically or paramilitarily.

Covert action has been the subject of much controversy both within and without the intelligence community. It has been a significant foreign policy tool and can continue to provide national policy makers with a regulated alternative for carrying out selected policy decisions by means not within the purview or capability of other agencies. For example, in 1991, President George H. W. Bush reportedly authorized the Central Intelligence Agency (CIA) to develop plans, including covert action, to block the proliferation of WMDs to the Third World.[51] More recently, the CIA played an important role in the U.S. invasion of Afghanistan to overthrow the Taliban regime in 2001.[52]

Despite its potential utility, there is a danger that unduly focusing on the covert action aspect of the broader intelligence scene can generate control mechanisms and create a climate, at home and abroad, of opinion prejudicial to the overall intelligence mission. Another danger lies in the fact that *covert action* is a very imprecise, elastic term. It covers everything from having lunch with a foreign journalist to encourage her to write an editorial that may well have been written anyway to running elaborate, large-scale paramilitary operations over time spans measured in years. It is therefore hard to discuss this concept in a rational, meaningful way—especially in a public forum.

Though clandestine activities have long been part of statecraft, only since the late 1970s have the mechanisms by which they are conducted and controlled come under close public scrutiny in the United States. When Congress created the CIA in 1947 to perform certain intelligence coordination functions, it directed the agency to also undertake "such other functions and duties related to intelligence affecting the national security as the President or the National Security Council may from time to time direct."[53] Since then, National Security Council (NSC) directives have given the CIA authority to conduct covert operations abroad consistent with American foreign and military policies.[54] Over time, Congress began to assert its oversight in this realm. An important step was the 1974 Hughes-Ryan Amendment, which required the CIA to report any planned action to the appropriate committees of Congress "in a timely manner."

By the early 1980s, following general public dissatisfaction over the inability to extricate American hostages from Iran during the Carter administration, the covert action function had regained a sense of vitality. This new trend toward a more fully developed covert action capability was short lived, however, as the consensus that had been building in support of covert action was severely weakened by the highly publicized 1985–1986 Iran-Contra affair. As a result of this

episode, new legislation was enacted and signed by George H. W. Bush in the summer of 1991 that required the president to give written approval for any covert action undertaken by any component of the U.S. government and to notify Congress in a timely fashion. In addition, the president must notify Congress when third countries or private citizens are to be used or take part in covert activity in any significant way.[55]

Although covert operations survive in theory as an important vehicle for foreign policy implementation in special cases, there is a real question about their future practicality. In addition to the challenge of preserving the secrecy necessary to their success, these operations are often risky in terms of lives as well as the costs their revelation can impose on the achievement of broader national security policy goals. As a twenty-first century example, questions about the existence and operations of a secret CIA prison system stirred up great controversy during the administration of President George W. Bush. Critics sought explanations as to why a clandestine detention system was superior to existing legal and open detention and interrogation practices.[56] In the process of responding to public and congressional inquiries, an administration may find it necessary to reveal information that made a secret program attractive in the first place. Controversies such as these may also negatively affect both domestic public support and the image of the United States abroad.

## Counterintelligence

Counterintelligence efforts attempt to deny real or potential adversaries the ability to collect information that can be used against the United States. Counterintelligence is one of the least understood and appreciated functions of the intelligence community. It has been defined as:

> the national effort to prevent foreign intelligence services and foreign-controlled political movements (which are often supported by intelligence services) from infiltrating our institutions and establishing the potential to engage in espionage, subversion, terrorism and sabotage. Counterintelligence involves investigations and surveillance activities to detect and neutralize the foreign intelligence presence, the collation of information about foreign intelligence services and the initiation of operations to penetrate, disrupt, deceive, and manipulate these services . . . to our advantage.[57]

In the current era, with foreign intelligence agencies in many cases focused on acquiring classified technological data and business and economic secrets, the definition of counterintelligence needs to be broadened to include frustration of foreign efforts to acquire sensitive information of all kinds.

Like covert action, counterintelligence operations often lead to controversy. There is general distrust of intelligence activities within the United States, yet this is precisely where counterintelligence officers must operate. This distrust is only heightened in the face of occasional revelations of agency misconduct. For example, in 2007, Robert Mueller, the director of the Federal Bureau of Investigation (FBI), was called before the Senate Judiciary Committee to explain failures on the

part of the FBI to appropriately manage "national security letters"—instruments that enable the FBI to obtain communications and financial records without initial court oversight.[58] Even when counterintelligence activities are flawlessly managed, they still raise sensitive issues relating to potential infringement on the liberties of U.S. citizens.

## Direction and Leadership of the Intelligence Community

The intelligence community is a collection of executive branch agencies and organizations that work both separately and together to conduct intelligence activities necessary for foreign relations and the protection of the national security of the United States.[59] Some knowledgeable observers, however, contend that the term *intelligence community* overstates the degree of cohesiveness in the American intelligence establishment. The community concept expresses the intent to get disparate entities to work together in sufficient harmony to develop the best possible intelligence products while avoiding excessive duplication of effort. The practical challenges associated with realizing that intent are formidable.

**Direction of the Intelligence Community.** The NSC is the highest executive branch entity (other than the president) providing direction to the national intelligence effort. The NSC announces the National Security Strategy and the national foreign intelligence objectives and priorities, which are then translated into specific guidance for the intelligence community. The NSC also reviews all proposals for special activities (i.e., covert actions), making recommendations on each to the president. In addition, it assesses proposals for sensitive intelligence collection operations and is aware of counterintelligence activities. Theoretically, the NSC evaluates the quality of the intelligence product as well. It is important to note that most of these missions are, in fact, accomplished by the national security staff acting under the direction of the assistant to the president for national security affairs or by a lower-level interdepartmental group. The NSC itself seldom provides specific direction to the intelligence effort.

**Leadership of the Intelligence Community.** The National Security Act of 1947 established the position of director of central intelligence (DCI) to lead the intelligence community in responding to executive direction and mandated that the head of the CIA would play that role. Although the DCI's position was progressively strengthened in the decades following 1947, management and coordination of the community as a whole remained problematic. The DCI had supervisory responsibility but did not have the authority to truly command the community and did not control the majority of the resources dedicated to the intelligence function.

The most significant change to the leadership of the intelligence community came after the 9/11 terrorist attacks on U.S. soil. One of the recommendations of the 9/11 Commission that investigated these attacks was to replace the DCI with a "National Intelligence Director" with two main responsibilities: "(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."[60] This recommendation led to the Intelligence Reform and Terrorism Prevention Act of 2004—the most significant legislative reform since the intelligence community's inception—which created the position of the Director of National Intelligence (DNI). As explained by George W. Bush when he signed the legislation into law in December 2004, the DNI:

> will serve as the principal advisor to the President on intelligence matters. The DNI will have the authority to order the collection of new intelligence, to ensure the sharing of information among agencies and to establish common standards for the intelligence community's personnel. It will be the DNI's responsibility to determine the annual budgets for all national agencies and offices and to direct how these funds are spent.[61]

The DNI now serves as the head of the intelligence community and acts as the principal advisor to the president, the NSC, and the Homeland Security Council for intelligence matters related to national security. The Office of the DNI also has within it the National Intelligence Council. This council provides the entire intelligence community with an independent analytical and estimative capability and also prepares national intelligence estimates using all the community's resources as well as nongovernmental experts.

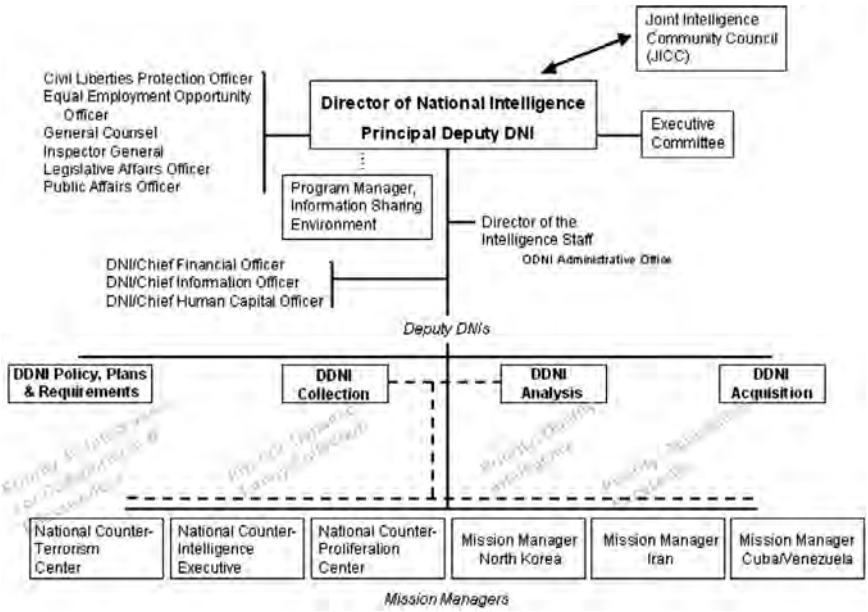
Although the creation of the DNI was a significant reform, the new position has weaknesses as well as strengths. Perhaps the two most significant strengths relate to resources and personnel. The DNI directs and oversees the creation of the National Intelligence Program—a role that gives the DNI control over the budgets for the national missions of the intelligence agencies. In terms of personnel, the DNI also has authority over community-wide personnel programs. This authority may enable the DNI to affect the career patterns and incentive structures of career intelligence officials to become supportive of community-wide goals.[62] However, the position of the DNI also contains major weaknesses. These concerns were summed up by Senator John Rockefeller in confirmation hearings for a new DNI in February 2007:

> We did not pull the technological collection agencies out of the Defense Department and we did not give the DNI direct authority over the main collection or analytical components of the community. We gave the DNI the authority to build the national intelligence budget, but we left the execution of the budget with the agencies. We gave the DNI tremendous responsibilities. The question is, did we give the position enough authority for him to exercise those responsibilities?[63]

Congress is likely to continue to assess this question for some time to come.

In addition to creating a stronger head of the intelligence community, another major reform directed by the Intelligence Reform and Terrorism Prevention Act of 2004 was the codification in law of the National Counter-Terrorism Center (NCTC). Established in 2003 by the president as the Terrorist Threat Integration Center, the president subsequently renamed it the NCTC in an August 2004 presidential executive order. Congress codified it in its 2004 legislation and placed it within the Office of the DNI (see Figure 7.2). The key purpose of this center is to ensure unity of effort within the intelligence community on an issue of critical

**FIG. 7.2** Structure of the Office of the Director of National Intelligence




*Source:* www.odni.gov/org_chart

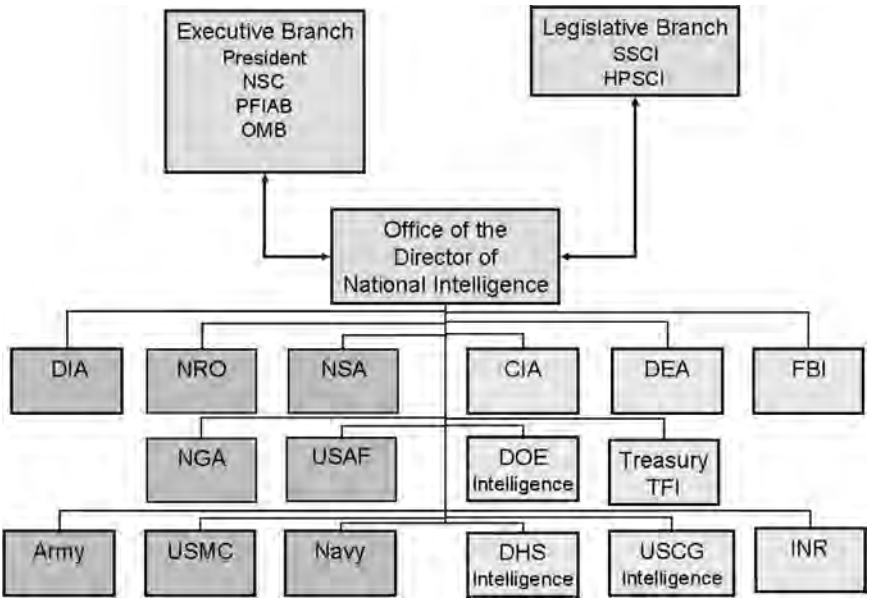
importance to national security. As with the role and effectiveness of the DNI, this organization and its functions are likely to continue to evolve. The 2004 act also provides for and seems to envision the creation of additional, similar centers focused on other key national security concerns. One, the National Counter-Proliferation Center, has already been established.

## Members of the Intelligence Community

The intelligence community within the United States currently has sixteen components that all fall under the oversight of the DNI. Of these entities, the CIA is the only one that is independent. All the others fall under executive departments within the government: eight within defense, two within homeland security, two within the Department of Justice, and three within other executive departments. These are listed in Figure 7.3 and will be discussed in turn below.

**Central Intelligence Agency.** The CIA collects information abroad and serves as the national manager for human source collection. It is the only agency within the community authorized to conduct covert activities, although the president can direct other agencies to be involved. Though its operations are conducted almost entirely outside the United States, it can participate in counterintelligence activities at home in support of the FBI, as well as in certain limited domestic activities that support overseas collection operations.

**FIG. 7.3** The Intelligence Community




*Source:* www.wmd.gov/report/wmd_report.pdf

**Department of Defense.** The importance of defense-related concerns to the intelligence community is reflected in the fact that half of its components reside within the DoD. Whereas the CIA serves primarily national consumers, these DoD components also serve military commanders at all levels. The importance of the intelligence entities within the DoD was reflected in Secretary of Defense Donald Rumsfeld's creation of the Office of the Undersecretary of Defense for Intelligence in 2003. (Earlier, intelligence was at the assistant secretary level.) The third-highest-ranking official in the Pentagon, the undersecretary of defense for intelligence is responsible for coordinating efforts within the defense intelligence community and serving as the focal point for interaction with the DNI and the rest of the intelligence community.[64]

*Defense Intelligence Agency.* Headquartered in the Pentagon, the DIA produces military and military-related intelligence for the DoD. The director of the DIA serves as the principal advisor on substantive military matters to the secretary of defense and the Joint Chiefs of Staff. The DIA also provides military input for national intelligence products and supervises the work of all military attachés abroad. Within DIA is also the Central MASINT Organization, the focus for all national and DoD MASINT matters.

*National Security Agency.* The National Security Agency (NSA), headquartered at Fort Meade, Maryland, has two main strategic missions. The first of these is to conduct signals intelligence (explained above), and the second is information

assurance. In this latter capacity, NSA "prevents America's adversaries from exploiting sensitive U.S. government communications by giving policy-makers and warfighters a secure means of communicating."[65] Because of the nature of its responsibilities, the NSA operates in the dynamic realm of information technology and must constantly adapt to be effective at its core missions.

*National Reconnaissance Office.* The National Reconnaissance Office (NRO) "develops and operates unique and innovative overhead reconnaissance systems and conducts intelligence related activities essential for U.S. national security."[66] Due to the sensitivity of its responsibilities, the existence and functions of the NRO were only declassified in September 1992. The NRO is jointly managed by the secretary of defense and the DNI, though it is the latter who establishes its requirements and collection priorities.[67]

*National Geospatial-Intelligence Agency.* The new National Geospatial-Intelligence Agency (NGA) replaced the National Intelligence Mapping Agency. The national manager for both classified and unclassified imagery products, it is also responsible for providing timely, relevant, and accurate GEOINT in support of military forces and national requirements.

*Army, Air Force, Navy, and Marine Corps Intelligence.* In addition to the above agencies, each of the armed services has intelligence and counterintelligence capabilities. These service component entities provide support to decision makers at tactical, operational, and strategic levels.

**Department of Homeland Security.** Two components of the intelligence community reside within the Department of Homeland Security (DHS). The first of these is the Office of Intelligence and Analysis, which is responsible for overseeing and integrating all the intelligence elements of the department (see Chapter 6 for the organizational structure of the DHS). The Office of Intelligence Analysis is also responsible for coordination between the DHS and state and local governments, the rest of the intelligence community, and Congress. The second component of the intelligence community within the DHS is Coast Guard Intelligence, which was transferred with the rest of the Coast Guard from the Department of Transportation when the DHS was created.

**Department of Justice.** Two components of the intelligence community are agencies within the Department of Justice. The first of these is the FBI. Although primarily a domestic investigative and law enforcement agency, the FBI has extensive domestic counterintelligence and security responsibilities. After the 9/11 terrorist attacks, the "overriding priority" of the FBI became "protecting America by preventing future attacks."[68] In 2005, George W. Bush directed the creation of a National Security Service in the FBI, and the agency responded by creating the

National Security Branch. Within this organization, FBI counterterrorism, counterintelligence, and intelligence functions all reside. The director of this branch also coordinates FBI national security efforts with the rest of the intelligence community. In addition to the National Security Branch, the FBI also fulfills its national security responsibilities through fifty-six field offices in major U.S. cities, over four hundred resident offices in smaller communities, and fifty offices located in embassies worldwide.[69]

The second component of the intelligence community within the Department of Justice is the Drug Enforcement Agency (DEA). The DEA's Office of National Security Intelligence "is responsible for providing drug-related information responsive to intelligence community requirements."[70] The DEA is experienced with operating in foreign environments and—with eighty-six offices in sixty-three countries—has the largest the U.S. law-enforcement agency presence abroad.[71]

**Department of State.** Diplomatic reporting is a valuable information-gathering resource. Representatives of the State Department stationed overseas regularly report to Washington regarding developments relevant to U.S. foreign policy, including information about foreign political, sociological, economic, and scientific trends or events. For the rest of the community as well as for the secretary of state, the department's Intelligence and Research Bureau generates intelligence products pertinent to U.S. foreign policy. The secretary of state works closely with the DNI, and the State Department with the CIA, to ensure that intelligence activities are both useful to and cognizant of American foreign policy.

**Department of the Treasury.** Treasury's Office of Intelligence Analysis, established in 2004, is a member of the intelligence community. Run by an assistant secretary and residing within the Office of Terrorism and Financial Intelligence, this office coordinates with the rest of the intelligence community and investigates such issues as nuclear proliferation financing and terrorism financing.[72]

**Department of Energy.** The Department of Energy participates with the State Department in overt collection of information on foreign energy matters, particularly nuclear energy, and also produces such intelligence as the secretary of energy may need to discharge the duties of the office. A particular value added of the Office of Intelligence and Counterintelligence within the Department of Energy is its ability to provide technical expertise when evaluating and helping to counter such threats as nuclear proliferation.

## Intelligence Oversight

Because there is no explicit provision in the Constitution for the control of intelligence, authority for it must be inferred from provisions for the national defense and foreign affairs functions that intelligence serves. As Congress shares power with the president in these functions, its claims to comparable authority in the

field of intelligence can be hard for the executive branch to counter. If congressional participation in foreign policy formulation and control is to be significant, Congress must have access to relevant information, providing it an additional incentive to take an active role in intelligence policy.

**Congressional Perspective and Actions.** From the enactment of the National Security Act of 1947 until about 1970, there existed a broad consensus on Capitol Hill that acknowledged the president's control of the intelligence community. By the early 1970s, however, that consensus had been eroded by the unfolding Watergate scandal and allegations concerning CIA involvement in Chilean presidential elections. Responding to these developments, Congress in 1974 passed the Hughes-Ryan Amendment to the Foreign Assistance Act. This legislation required that the president, prior to the expenditure of appropriated funds for noncollection intelligence activities in foreign countries, issue a "finding" that declared the activity to be "important to the national security" of the United States and report this finding to appropriate congressional committees. Subsequently, both the House and Senate launched investigations into alleged CIA misconduct.

Although the respective committees operated concurrently, the Senate committee (known as the Church Committee after its chairman, Senator Frank Church) took the lead. Its investigatory charter was broad and open ended, instructing the committee to measure intelligence activities against standards of both legality and propriety. After examining records, listening to witnesses, and deliberating at length, the committee decided that the United States had been implicated in several political assassination plots. Operational authorization procedures within the intelligence community seemed so deliberately compartmented and secretive that a plan to kill a foreign leader could be generated without explicit presidential approval. Much of the public debate on this matter, however, missed an important point. The president had been deliberately insulated from formal involvement in covert actions, not to keep him ignorant of them, but to allow him to take the public line that the chief of state was not involved.

The committee's final report called for adherence to "fair play" ideals. The committee clearly believed that the looseness of operational rules and discretion had sometimes led to intelligence operations resembling those of the country's totalitarian competitors. Remedies suggested by the committee included clear legislative delineation of the scope of permissible activities (via a statutory charter for the intelligence community) and better procedures for supervising intelligence agency operations (including more and better congressional oversight).

After the completion of these investigations, Congress had before it two self-imposed tasks: to put its oversight machinery in order and to pass legislative charters setting forth authorizations and restrictions for the intelligence community. The Senate Select Committee on Intelligence (SSCI) was created in 1976, and the House Permanent Select Committee on Intelligence (HPSCI) followed in 1977. In a 1977 report, the SSCI stated its intent to serve congressional and constitutional interests in the following ways:

1. *Obtain information relevant to foreign policy decisions.* The select committee was instructed by the Senate to "provide informed and timely intelligence necessary for the executive and legislative branches to make sound decisions affecting the security and vital interests of the nation." Access to intelligence products became a matter of institutional right.
2. *Use the budget process as a control mechanism.* During the committee's first year, it helped prepare legislation specifically authorizing appropriations for all aspects of intelligence, including a project-by-project review of covert action. This review procedure was a major step beyond the past, when intelligence monies were hidden throughout the budget, and opened the way for far more congressional influence than had been felt before in the intelligence arena.
3. *Control by investigation.* In its first year, the Senate committee investigated one hundred allegations of improprieties. The role of Congress as an institutional inquisitor is a well-established one.
4. *Review of covert operations proposals.* An oversight procedure established in conjunction with the executive branch gave the Senate committee what amounted to an approval role in covert action operations. Once the president approves a proposal, the committee is informed. Should the committee feel that pursuit of a covert action would not be in the best interests of the country, its procedures provide for taking the issue to the Senate in closed session. The rules even envisioned disclosure of facts concerning the operation, if confrontation over its advisability persisted.

Work on a statutory charter for the intelligence community proved more difficult than the provision of oversight. After other proposals failed, the Intelligence Oversight Act of 1980 was enacted. This law repealed the Hughes-Ryan Amendment and reduced the number of congressional oversight committees to the two select committees on intelligence. A 1991 amendment to this act defined covert activities and required written approval by the president in advance; it also stipulated that the intelligence committees in Congress be informed as the activities proceeded.[73]

Congressional scrutiny of intelligence operations was strengthened by the 1978 Foreign Intelligence Surveillance Act (FISA). This act required judicial warrants for electronic intelligence surveillance used in intelligence and counterintelligence operations within the United States whenever communications of "United States persons" might be intercepted. This act also created the Foreign Intelligence Surveillance Court, where the judges maintain sufficient clearances to hear the compartmentalized intelligence that supports probable cause warrants for foreign agents.

In the 1980s, there was a lull in legislation despite high-profile actions by members of the intelligence community. The foremost among these were CIA covert actions, such as the mining of Nicaraguan waters and the Iran-Contra scandal. Although the latter incident created a spectacle, it did not lead to any significant restrictions.

In the 1990s, Congress created the bipartisan Commission on Roles and Capabilities of the U.S. Intelligence Community through the Intelligence Authorization

Act of fiscal year 1995. The Commission analyzed the new threats facing the United States after the Cold War and found that improvements were needed in several areas to include community interaction, cost and burden sharing with allies, and public relations.[74]

After the attacks of 9/11, the federal government took another hard look at itself. One result was the creation of the DHS, discussed in Chapter 6. Congress and the president also created the 9/11 Commission and chartered it broadly "to investigate facts and circumstances relating to the terrorist attacks of September 11, 2001," including those that were related to the intelligence community.[75] The 9/11 Commission identified inadequate communication between law enforcement and intelligence agencies, and among members of the intelligence community, to be significant problems.

As discussed above, the Intelligence Reform and Terrorism Prevention Act of 2004 responded to some of these recommendations by establishing the DNI and creating the NCTC to integrate the intelligence effort on high-priority intelligence threats. In addition, the 2004 law created an independent Privacy and Civil Liberties Board. Working as a part of the Executive Office of the president and led by a chair and vice chair, both of whom must be confirmed by the Senate,[76] it ensures the civil liberties of American citizens are not infringed upon by laws, policies, or decisions of the executive branch.[77]

**Executive Oversight.** In addition to congressional oversight mechanisms, the executive branch has its own oversight entities and procedures. One entity that presidents have used to exercise oversight over the intelligence community is the President's Foreign Intelligence Advisory Board (PFIAB). Established in 1956 by President Dwight Eisenhower as the President's Board of Consultants, PFIAB has had an on-again, off-again existence since the 1960s. Currently consisting of eleven members, the PFIAB has no line authority, but because it reviews all intelligence activities with a special responsibility for the quality of products and management, and because it reports to the president at least semiannually, it has an important role.

As noted above, allegations of intelligence community abuses—both domestic and abroad—generated considerable concern in the United States in the 1970s. As a result, additional procedures to preclude unauthorized activities were instituted. The President's Intelligence Oversight Board (PIOB), a three-member panel of private citizens appointed by the president, was created by President Jimmy Carter in 1976 to review and report to the president on the intelligence community's internal procedures and operational activities. Within the intelligence community itself, inspectors general and general counsels were specifically made responsible to report to the PIOB on all potential breaches of the law by their agencies. As part of an effort to streamline his office, President Bill Clinton eliminated the PIOB in 1993 and transferred its responsibilities to a committee of the PFIAB. This action eliminated an important safeguard when it erased the direct reporting line to the president.

Executive oversight has varied over time in intensity and effectiveness. Reflecting his concern for reinvigorating the capability of the intelligence community to

deal with a wide array of national security threats, President Ronald Reagan, by executive order, provided a strengthened new charter for the community. Unfortunately, the climate created by this executive order, as well as the activities of his influential and strong-minded DCI, William Casey, led to a number of excesses. These included the CIA's mining of Nicaraguan waters without informing Congress and the Iran-Contra scandal. These episodes, in turn, led to congressional investigations, a call for more restrictions on the CIA, and the 1987 appointment of a highly respected, nonpolitical outsider, William Webster, as DCI. (Webster had earlier headed the FBI.)

As is evident from this condensed historical survey, the executive branch not only directs the intelligence community but also seeks independent mechanisms for ensuring oversight. Because administrations take different approaches to the intelligence community, interspersed periods of more and less restrictive executive branch oversight are likely to continue. Given this factor, as well as the nature of the intelligence function and the continuously changing national security environment, both branches of government are likely to continue to reassess and readjust their mechanisms for exercising intelligence oversight.

**Judicial Oversight.** Judicial oversight of the intelligence community has been historically minor, primarily because most intelligence activities take place overseas and are directed against foreign nationals or nations. Arguably, the initial interaction of the judiciary and the intelligence community was the use of wiretaps by law enforcement agencies and the Supreme Court's 1967 decision in *Katz v. United States*. In this case, the Court held that Katz had a reasonable expectation of privacy that society was prepared to recognize in his phone-booth conversations.[78] This case overruled an earlier (the Olmstead) case that stated if there was not a physical invasion into a constitutionally protected space, there was no need for a warrant.

The aftermath of the Watergate scandal and revelations of the recording of personal communications without warrants fueled the public's desire to see all warrants governed by a legal process. The 1978 FISA legislation authorized the Chief Justice of the United States to designate seven federal district court judges to review applications for warrants related to national security investigations within a Foreign Intelligence Surveillance Court.[79] FISA also requires that a court order or warrant be obtained from this court for all electronic surveillance for intelligence purposes within the United States.[80] Warrant applications under FISA are drafted by attorneys in the General Counsel's Office at the NSA at the request of an officer of one of the federal intelligence agencies. Each application must contain the attorney general's certification that the target of the proposed surveillance is either a "foreign power" or "the agent of a foreign power" and, in the case of a U.S. citizen or resident alien, that the target may be involved in the commission of a crime.[81]

The first change to FISA came as a result of the Patriot Act. Perhaps the most significant provisions of the Patriot Act were those intended to lower the barriers blocking cooperation between intelligence and law enforcement by lowering the

threshold for getting a surveillance warrant, expanding the ability of the FBI to gather information without a warrant, and expanding surveillance on the Internet. In addition, it expanded the time periods for which the Foreign Intelligence Surveillance Court can authorize surveillance and increased the number of judges serving the court from seven to eleven.[82] George W. Bush's controversial authorization of warrantless wiretaps by the NSA on international calls in 2001, avoiding FISA procedures as too cumbersome and lengthy, constitutes another arena in which judicial oversight and presidential prerogative clash.

Though judicial oversight is not unimportant, the judiciary is limited to the realm of legal interpretation. This is in sharp contrast to Congress, which has the ability to subpoena, address policy issues, and control the funding for elements of the intelligence community.[83]

## Looking Ahead

As is evident in this chapter, today's intelligence community operates in a challenging and dynamic environment. In addition to the complexity of the international security environment and the dynamism of modern technology, many elements within the intelligence community have experienced at least some degree of organizational change in response to the lessons of 9/11. Due to the recent nature of some of these changes, such as the creation of the DNI and the NCTC, the significance of these reforms and their impact on the quality of the U.S. intelligence effort remains to be seen.

In the midst of these developments, the intelligence community suffered a significant blow to its reputation with the failure to discover its predicted WMDs in Iraq after the 2003 U.S.-led invasion. In the words of the "Weapons of Mass Destruction Commission" report:

> On the brink of war, and in front of the whole world, the United States asserted that Saddam Hussein had reconstituted his nuclear weapons program, had biological weapons and mobile biological weapons 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.[84]

The commission acknowledged the difficulty of the intelligence problem that WMDs pose but nevertheless found that this major intelligence failure was also the product of shortcomings in collection, analysis, and the manner in which available intelligence was made available to policy makers. The related question of how policy makers used assessments that were provided to them by the intelligence community has yet to be similarly investigated.[85]

As the intelligence community continues to evolve, one thing is clear: It will continue to be held accountable to both the president and Congress. Without cooperation with and from both branches, the community will not be able to acquire the resources or authorizations it needs to operate effectively. In addition, given the importance of counterterrorism and concern about homeland security, the role played by judicial oversight of the intelligence process is likely to increase. The way ahead is challenging.

## Discussion Questions

1. What is intelligence, and what contribution does the intelligence community make to the national security decision-making process?
2. How is the intelligence community structured? Who leads the intelligence community?
3. How did the events of 9/11 help shape the current structure?
4. What resources are used in OSINT? How important is OSINT to the U.S. intelligence effort?
5. In what ways can bias impact analysis? How can policy makers and the intelligence community guard against the effects of bias?
6. How has oversight over the intelligence community changed over the years? Which branches of the government maintain oversight today?
7. With an increased focus on nonstate actors in the current international security environment, what types of intelligence collection will become most important?
8. Should covert action remain an important instrument of U.S. national security policy? What are the strengths and weaknesses of this policy tool?

## Recommended Reading

Andrew, Christopher. *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush.* New York: Harper Perennial, 1996.

Cilluffo, Frank J., Ronald A. Marks, and George C. Salmoiraghi. "The Use and Limits of U.S. Intelligence." *Washington Quarterly* 25, no. 1 (2002): 61–74.

Clark, Robert M. *Intelligence Analysis: A Target-Centric Approach*. 2nd ed. Washington, DC: CQ Press, 2007.

Dupont, Alan. "Intelligence for the Twenty-first Century." *Intelligence and National Security* 18, no. 4 (Winter 2003): 15–39.

George, Roger Z., and Robert D. Kline. *Intelligence and the National Security Strategist: Enduring Issues and Challenges.* Washington, DC: NDU Press, 2004.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 3rd ed. Washington, DC: CQ Press, 2006.

National Commission on Terrorist Attacks. *The 9/11 Commission Report.* New York: W. W. Norton & Company, 2004.

Odom, William E. *Fixing Intelligence: For a More Secure America.* New Haven, CT: Yale University Press, 2003.

Scott, Len, and Peter Jackson. "The Study of Intelligence in Theory and Practice." *Intelligence and National Security* 19, no. 2 (June 2004): 139–169.

Shulsky, Abram N., and Gary L. Schmitt. *Silent Warfare: Understanding the World of Intelligence*. 3rd ed. Washington, DC: Brassey's, 2002.

Stiefler, Todd. "CIA's Leadership and Major Covert Operations: Rogue Elephants or Risk-Averse Bureaucrats?" *Intelligence and National Security* 19, no. 4 (Dec 2004): 632–654.

Taylor, Stan, and David Goldman. "Intelligence Reform: Will More Agencies, Money, and Personnel Help?" *Intelligence and National Security* 19, no. 3 (Sept 2004): 416–435.

Treverton, Gregory F. *The Next Steps in Reshaping Intelligence.* Santa Monica, CA: RAND Corporation, 2005.

## Internet Sources

Central Intelligence Agency Center for the Study of Intelligence, www.cia.gov/library/center-for-the-study-of-intelligence/index.html
Office of the Director of National Intelligence, www.odni.gov
President's Intelligence Advisory Board, www.whitehouse.gov/pfiab
U.S. House of Representatives Permanent Select Committee on Intelligence, http://intelligence.house.gov
U.S. Intelligence Community, www.intelligence.gov/index.shtml
U.S. Senate Select Committee on Intelligence, http://intelligence.senate.gov