Challenge Your Understanding

The following questions are designed to challenge your understanding of the material presented in this chapter. Some questions may require additional research outside this book in order to provide a complete answer.

1. For most of U.S. history, who was the single individual who coordinated national security?
2. Why was the National Security Council formed after World War II?
3. Who are the statutory members of the National Security Council?
4. Who is the chief military advisor to the President?
5. Who is the chief intelligence advisor to the President?
6. What is the function of the National Security Advisor?
7. What is the function of the National Security Staff?
8. What is the designation of the NSC senior policy group?
9. What is the designation of the NSC policy groups that are the main forum for interagency coordination?
10. List and describe at least two potential pitfalls of the NSC system.

Chapter 37

Intelligence Community

Learning Outcomes

Careful study of this chapter will help a student do the following:

- Define the term “intelligence”.
- Discuss the purpose and performance of the CIA prior to 2004.
- Compare the authorities of the ODNI and CIA.
- Identify different members of the Intelligence Community.
- Identify different intelligence disciplines.
- Describe the intelligence cycle.
- Explain the necessary predicate for conducting surveillance of U.S. citizens.

"Since the Pearl Harbor attack of 1941, the intelligence community has devoted generations of effort to understanding the problem of forestalling a surprise attack."

- 2004 9/11 Commission Report

Introduction

The U.S. Intelligence Community (IC) is a coalition of 17 agencies and organizations, within the Executive Branch that work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities. [1]

The United States has carried out intelligence activities since the days of George Washington, but only since World War II have they been coordinated on a government-wide basis.

Background

Intelligence is secret, state activity to understand or influence foreign entities. [2] The United States has carried out intelligence activities since the days of George Washington, but only since World War II have they been coordinated on a government -wide basis. President Franklin D. Roosevelt appointed New York lawyer and war hero, William J. Donovan, to become first the Coordinator of Information, and then, after the U.S. entered World War II, head of the Office of Strategic Services (OSS) in 1942. The OSS had a mandate to collect and analyze strategic information. After World War II, however, the OSS was abolished along with many other war agencies and its functions were transferred to the State and War Departments. [3]

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." [4]

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. [4]

As the head of the CIA, the Director of Central Intelligence (DCI) served as the principal adviser to the President for intelligence matters related to national security. According to the 1947 National Security Act, such national intelligence was to be timely, objective, independent of political considerations, and based upon all sources available to the Intelligence Community. To coordinate the efforts of the Intelligence Community, the DCI was given authority over a National Intelligence Council (NIC), comprised of senior analysts from the Intelligence Community and substantive experts from the public and private sector. The focus of the National Intelligence Council was to produce National Intelligence Estimates (NIEs) for the Government. To enforce cooperation among the Intelligence Community, the National Security Act of 1947 made the DCI the "Head of the Intelligence Community" responsible for 1) developing and presenting the annual budget for National Foreign Intelligence Programs; 2) establishing requirements and priorities for the collection of intelligence by elements of the IC; and 3) approving collection priorities for national collection assets. [5]

The establishment of the CIA was borne out of a collective failure to anticipate Japan's attack on the U.S. Pacific Fleet at Pearl Harbor that led to America's entry into World War II. Now engaged in a Cold War to contain further expansion of the Soviet Union, a primary objective of the CIA was to prevent an "Atomic Pearl Harbor" that could lead to World War III.

The establishment of the CIA was borne out of a collective failure to anticipate Japan's attack on the U.S. Pacific Fleet at Pearl Harbor that led to America's entry into World War II. Now engaged in a Cold War to contain further expansion of the Soviet Union, a primary objective of the CIA was to prevent an "Atomic Pearl Harbor" that could lead to World War III. A number of significant "intelligence failures" over the ensuring decades led some to question whether the CIA had the requisite authority to effectively coordinate the efforts of the Intelligence Community.

- In April 1961, a CIA-planned effort by Cuban exiles to overthrow Fidel Castro's regime and replace it with a non-communist, U.S.-friendly government went horribly awry when an aerial attack on Cuba's air force flopped and the 1,400-strong "Assault Brigade 2506" came under heavy fire from the Cuban military after landing off the country's southern coast. The botched invasion poisoned U.S.-Cuban relations.
- On Jan. 31, 1968, during the Tet holiday in Vietnam, North Vietnam's communist forces stunned the United States by launching a massive, coordinated assault against South Vietnam. While the communist military gains proved fleeting, the Tet Offensive was arguably the most decisive battle of Vietnam. Americans grew disillusioned with the war, prompting U.S. policymakers to shift gears and focus on reducing America's footprint in Vietnam.
- While the CIA accurately analyzed the Six-Day War between Israel and neighboring Arab states in 1967, it was caught flat-footed only six years later when Egyptian and Syrian forces launched coordinated attacks on Israeli forces in the Sinai Desert and the Golan Heights during the Jewish holiday of Yom Kippur. The conflict, which ended with a ceasefire in October 1973, tested U.S.-Soviet relations and pushed the Arab-Israeli conflict to the top of Washington's foreign-policy agenda.

- In August 1978, six months before the U.S-backed Shah Mohammed Reza Pahlavi fled Iran, the CIA infamously concluded that "Iran is not in a revolutionary or even a pre-revolutionary situation." Subsequently, the Ayatollah Ruhollah Khomeini rose to power in the Islamic Revolution of 1979, opening up a rift between Iran and the United States that persists to this day.
- The Soviet Union's military incursion into Afghanistan, which began in December 1979 and devolved into a bloody, nine-year occupation, took the Carter administration by surprise. The U.S. intelligence community had assumed that the specter of a costly quagmire would deter the Soviets from invading Afghanistan. Former CIA official Douglas MacEachin recalls that in the days after the invasion, a dark joke began circulating around the agency that "the analysts got it right, and it was the Soviets who got it wrong."
- Conventional wisdom holds that the U.S. intelligence community failed to predict the Soviet Union's demise in 1991, presaged as it was by President Mikhail Gorbachev's reforms, the deteriorating Soviet economy, the collapse of communism in east-central Europe, and the moves toward independence by several Soviet republics. As the BBC recently noted, "the Soviet example illustrates the problem that intelligence gatherers are great counters: they can look at missiles, estimate the output of weapons factories, and so on. But the underlying political and social dynamics in a society are much harder to read." [6]

Given a number of high-profile intelligence failures over the years, many outside observers argued that the DCI position was unworkable. They contended that DCIs, frustrated by the challenges involved in managing the entire intelligence community, focused narrowly on the CIA, and that the result was an ill-coordinated intelligence effort that poorly served the nation.

Many outside observers, Members of Congress, and various commissions over the years argued that the DCI position was unworkable. They contended that DCIs, frustrated by the challenges involved in managing the entire intelligence community, focused narrowly on the CIA, and that the result was an ill-coordinated intelligence effort that poorly served the nation. Some also asserted that DCIs lacked adequate legal authorities to establish priorities and to ensure compliance by intelligence agencies beyond the CIA. In particular, it was suggested that major intelligence agencies in the Department of Defense (DOD)—the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the National Geospatial-Intelligence Agency (NGA)—had been more responsive to the needs of the military services than to the requirements of national policymakers. And, finally, some observers, while conceding that DCI authorities under the National Security Act were limited, nevertheless contended that DCIs failed to fully assert their authorities, particularly when their priorities conflicted with those of the Secretary of Defense, viewed by many as the dominant voice in the intelligence community because of the Secretary's control over an estimated 85% of the intelligence budget. [7, p. 1]

Ultimately, it was the failure to anticipate 9/11 that prompted Congress to enact reform. In its report on the terrorist attacks of Sept. 11, 2001, the 9/11 Commission noted that the Intelligence Community, assailed by "an overwhelming number of priorities, flat budgets, an outmoded structure, and bureaucratic rivalries," had failed to pin down the big-picture threat posed by "transnational terrorism" throughout the 1990s and up to 9/11. [6] In response, Congress approved significantly larger intelligence budgets and, in December 2004, passed the most extensive reorganization of the intelligence community since the National Security Act of 1947. The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) created a new Director of National Intelligence to head the Intelligence Community, and serve as the principal intelligence adviser to the President, and oversees and directs the acquisition of major collections systems. [8, p. 1]

The 2004 Intelligence Reform Act assigned to the Director of National Intelligence (DNI) two of the three principal responsibilities formerly performed by the Director of Central Intelligence. The DNI would provide intelligence to the President, other senior officials, and Congress, and the DNI would head the Intelligence Community. The 2004 Intelligence Reform Act further strengthened the DNIs authority by providing enhanced budget authorities that were unavailable to the DCI.

Office of the Director of National Intelligence

The 2004 Intelligence Reform Act was designed to address the findings of the 9/11 Commission that there had been inadequate coordination of the national intelligence effort and that the Intelligence Community, as then organized, could not serve as an agile information gathering network in the struggle against international terrorists. [8, p. 1] The resulting Office of the Director of National Intelligence (ODNI) was consequently commissioned to improve information sharing, promote a strategic, unified direction, and ensure integration across the U.S. Intelligence Community. The ODNI stood up on April 21, 2005. [9, p. 15]

The 2004 Intelligence Reform Act assigned to the Director of National Intelligence (DNI) two of the three principal responsibilities formerly performed by the Director of Central Intelligence. The DNI would provide intelligence to the President, other senior officials, and Congress, and the DNI would head the Intelligence Community. But, unlike the DCI, the DNI would not oversee the CIA. Rather, the act renamed the DCI the DCIA, and subordinated their position to the DNI. [8, p. 2]

The 2004 Intelligence Reform Act further strengthened the DNIs authority by providing enhanced budget authorities that were unavailable to the DCI.

- First, it provides that at the DNI's exclusive direction, the Director of the Office of Management and Budget (OMB) shall "apportion," or direct, the flow of congressionally appropriated funds from the Treasury Department to each of the Cabinet level agencies containing intelligence community elements. This change is designed to strengthen the DNI's control over intelligence community spending. If, for example, an agency fails to comply with certain of the DNI's spending priorities, the DNI can withhold that agency's funding. DCIs had no such authority.

- Second, the DNI is authorized to "allot" or "allocate" appropriations directly at the sub-Cabinet agency and department level, providing the DNI additional control over spending. If a departmental comptroller refuses to act in accordance with a DNI spending directive, the law requires that the DNI notify Congress of such refusal. The DCI had no such authority or reporting obligation.
- Third, the DNI is authorized to "develop and determine" the National Intelligence Program (NIP; former "NFIP") budget. By contrast, DCIs were authorized to "facilitate the development" of the intelligence community's annual budget.
- Fourth, the DNI is authorized to "ensure the effective execution of the budget," and to monitor its implementation and execution. Except in the case of the CIA, DCIs had no such authority.
- Fifth, the DNI is authorized to provide budget guidance to those elements of the Intelligence Community not falling within the NIP. Again, DCIs had no such authority. [8, p. 6]

To assist with accomplishing its mission, the 2004 Intelligence Reform Act gave ODNI statutory authority over the National Counterterrorism Center (NCTC), National Counterproliferation Center (NCPC), the National Counterintelligence Executive (NCIX), and the National Intelligence Council.

The 2004 Intelligence Reform Act also authorized the DNI to "manage and direct the tasking of, collection, analysis, production, and dissemination of national intelligence ... by approving requirements and resolving conflicts." Although DCIs were authorized to exercise certain collection authorities, statutory authorities did not explicitly address analysis, production, and dissemination authorities. [8, p. 8]

To assist with accomplishing its mission, the 2004 Intelligence Reform Act gave ODNI statutory authority over the National Counterterrorism Center (NCTC), National Counterproliferation Center (NCPC), the National Counterintelligence Executive (NCIX), and the National Intelligence Council. [9, p. 15]

The National Counterterrorism Center has primary responsibility within the U.S. Government for counterterrorism intelligence analysis and counterterrorism strategic operational planning. NCTC's components are the Directorate of Intelligence, Directorate of Strategic Operational Planning, Directorate of Operations Support, Directorate of Terrorist Identities, and the Office of National Intelligence Management. Their functions are:

- Directorate of Intelligence leads the production and integration of counterterrorism analysis for the U.S. Government.
- Directorate of Strategic Operational Planning directs the U.S. Government's planning efforts to focus all elements of national power against the terrorist threat.
- Directorate of Operations Support provides the common intelligence picture for the counterterrorism community with 24 hours a day/7 days a week situational awareness; terrorism threat reporting; management and incident information tracking; and support for worldwide, national, and international special events.

- Directorate of Terrorist Identities maintains a consolidated repository of information on international terrorist identities and ensures Federal agencies can access the information they need through the Terrorist Identities Datamart Environment (TIDE).
- Office of National Intelligence Management provides strategic management of all national intelligence related to the IC's counterterrorism mission to set analytic and collection priorities; advance analytic tradecraft and training; and lead strategic planning, evaluation, and budgeting. [9, p. 16]

The National Counterproliferation Center is the bridge from the IC to the policy community for activities within the U.S. Government associated with countering the proliferation of weapons of mass destruction (WMD). NCPC conducts strategic counterproliferation planning for the IC to support policy efforts to prevent, halt, or mitigate the proliferation of WMDs, their delivery systems, and related materials and technologies. This includes both states of concern and, in partnership with the National Counterterrorism Center, non-state actors. NCPC achieves this by drawing on the expertise of counterproliferation professionals in the IC, the U.S. Government, industry, and academia. These relationships foster an atmosphere of collaboration and intelligence sharing in order to protect the U.S.'s interests at home and abroad. [9, pp. 16-17]

The National Counterproliferation Center is the bridge from the IC to the policy community for activities within the U.S. Government associated with countering the proliferation of weapons of mass destruction (WMD).

The National Counterintelligence Executive (NCIX) serves as the head of national counterintelligence and security for the U.S. Government. Per the Counterintelligence Enhancement Act of 2002, the NCIX is charged with promulgating an annual strategy for all counterintelligence elements of the U.S. Government. The Office of the NCIX is charged with integrating the activities of all counterintelligence programs to make them coherent and efficient. They also coordinate counterintelligence policy and budgets to the same end. It is also responsible for evaluating the performance of the counterintelligence community against the strategy. NCIX's Special Security Division is responsible for security policy and uniformity across the U.S. Government. [9, p. 17]

The National Intelligence Council (NIC), a Congressionally-mandated council, is a component of the ODNI that conducts mid- and long-term strategic analysis through the use of all-source intelligence. Since its formation in 1979, the NIC has been a source of deep substantive expertise on intelligence matters and a facilitator of integrated, IC coordinated strategic analysis on issues of key concern to senior U.S. policymakers. Some of the NIC's core functions are to:

- Produce National Intelligence Estimates — the IC's most authoritative written assessments on national security issues, as well as a broad range of other Community coordinated products.

- Foster outreach to nongovernmental experts in academia and the private sector to broaden the IC's perspective.

Articulate substantive intelligence priorities to guide intelligence collection and analysis. [9, p. 17]

The core mission of the ODNI is to lead the IC in Intelligence Integration, forging a community that delivers the most insightful intelligence possible. Intelligence Integration is the key to ensuring that the highest quality of intelligence is delivered with the right inputs, at the right time, in defense of the Homeland. [9, p. 15]

The core mission of the ODNI is to lead the IC in Intelligence Integration, forging a community that delivers the most insightful intelligence possible.

The Intelligence Community

The Director of National Intelligence is responsible for coordinating the combined efforts of the Intelligence Community. The IC is defined in 50 U.S.C. 401a(4) as consisting of the following:

1. The Office of the Director of National Intelligence (ODNI)
2. Central Intelligence Agency (CIA)
3. Bureau of Intelligence and Research, Department of State (INR)
4. Defense Intelligence Agency (DIA)
5. National Security Agency (NSA)
6. National Reconnaissance Office (NRO)
7. National Geospatial-Intelligence Agency (NGA)
8. The National Security Branch, Federal Bureau of Investigation (FBI)
9. Army Intelligence
10. Navy Intelligence
11. Air Force Intelligence
12. Marine Corps Intelligence
13. Coast Guard Intelligence
14. The Office of Intelligence and Analysis, Department of the Treasury
15. The Office of Intelligence, Department of Energy
16. The Office of National Security Intelligence, Drug Enforcement Administration (DEA)
17. The Office of Intelligence and Analysis, Department of Homeland Security [8, p. 2]

Except for the CIA, intelligence offices or agencies are components of Cabinet departments with other roles and missions. The intelligence offices/agencies, however, participate in intelligence community activities while supporting the other efforts of their departments. [8, p. 2]

The CIA remains the keystone of the analytic efforts of the intelligence community. It has all-source analytical capabilities that cover the whole world outside U.S. borders. It produces a range of studies that address virtually any topic of interest to national security policymakers. The CIA also collects intelligence with human sources and, on occasion, undertakes covert actions at the direction of the President. (A covert action is 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.) [8, p. 2]

The CIA remains the keystone of the analytic efforts of the intelligence community. It has all-source analytical capabilities that cover the whole world outside U.S. borders. It produces a range of studies that address virtually any topic of interest to national security policymakers. The CIA also collects intelligence with human sources and, on occasion, undertakes covert actions at the direction of the President.

Three major national-level intelligence agencies in the Department of Defense—the National Security Agency, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency—absorb the larger part of the national intelligence budget. NSA is responsible for signals intelligence and has collection sites throughout the world. The NRO develops and operates reconnaissance satellites. The NGA prepares the geospatial data—ranging from maps and charts to sophisticated computerized databases—necessary for humanitarian operations and for targeting in an era in which military operations are dependent upon precision-guided weapons. In addition to these three agencies, the Defense Intelligence Agency (DIA) is responsible for defense attachés and for providing DOD with a variety of analytical products. It serves as the premier all-source analytic unit within DOD. Although the Intelligence Reform Act provides extensive budgetary and management authorities over these agencies to the DNI, it does not revoke the responsibilities of the Secretary of Defense for these agencies. [8, pp. 2-3]

The State Department's Bureau of Intelligence and Research (INR) is one of the smaller components of the intelligence community but is widely recognized for the high quality of its analysis. INR is strictly an analytical agency; diplomatic reporting from embassies, though highly useful to intelligence analysts, is not considered an intelligence function (nor is it budgeted as one). [8, p. 3]

The key intelligence functions of the FBI relate to counterterrorism and counterintelligence. The former mission has grown enormously in importance since September 2001, many new analysts have been hired, and the FBI has been reorganized in an attempt to ensure that intelligence functions are not subordinated to traditional law enforcement efforts. Most importantly, law enforcement information, including counterterrorism and counterintelligence information, is now expected to be

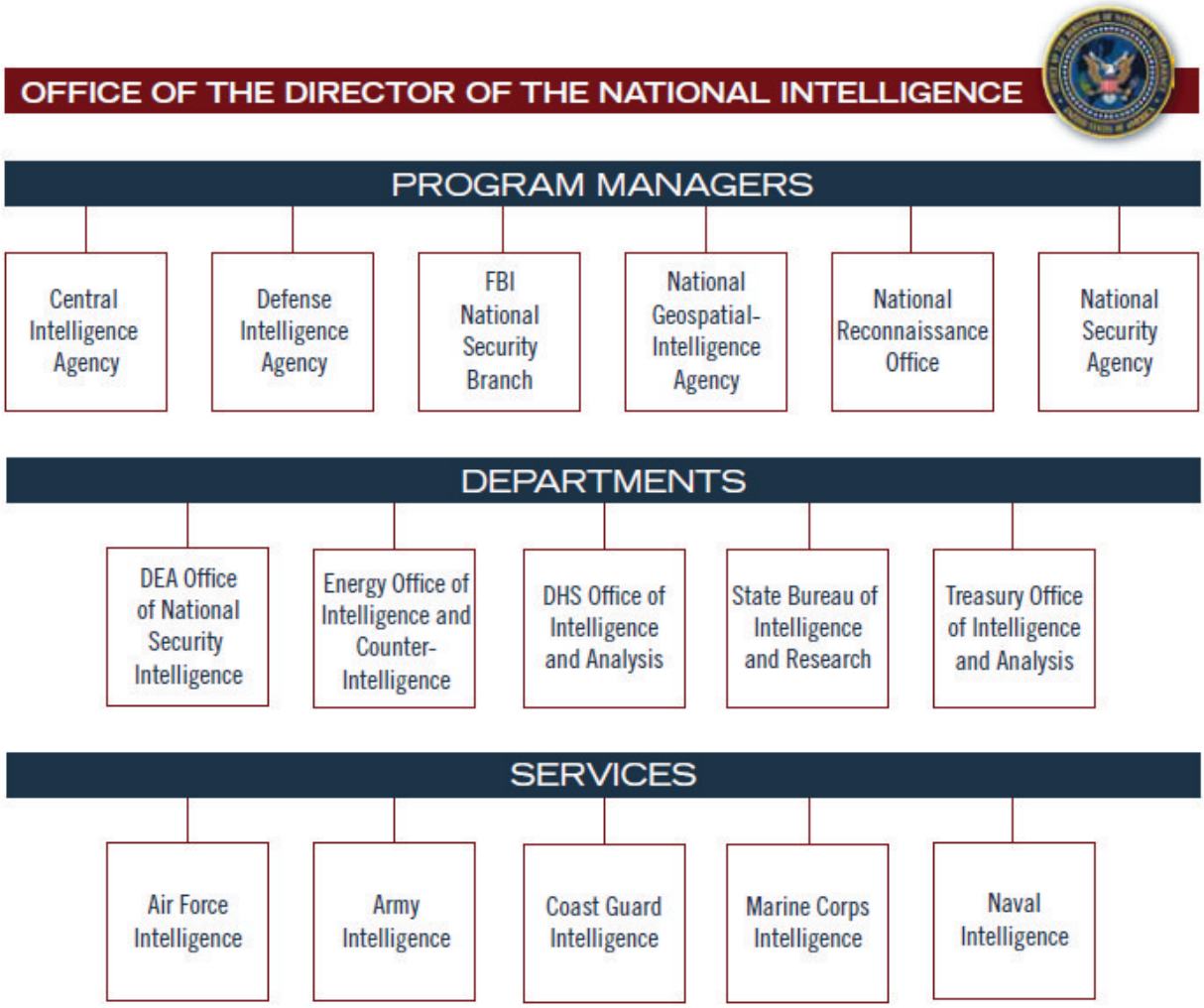

Figure 37-1: The U.S. Intelligence Community [9]

forwarded to other intelligence agencies for use in all-source products. The intelligence organizations of the four military services concentrate largely on concerns related to their specific missions. Their analytical products, along with those of DIA, supplement the work of CIA analysts and provide greater depth on key military and technical issues. [8, p. 3]

The intelligence organizations of the four military services concentrate largely on concerns related to their specific missions. Their analytical products, along with those of DIA, supplement the work of CIA analysts and provide greater depth on key military and technical issues. [8, p. 3]

The Homeland Security Act (P.L. 107-296) provided the Department of Homeland Security (DHS) responsibilities for fusing law enforcement and intelligence information relating to terrorist threats to the homeland. The Office of Intelligence and Analysis in DHS participates in the inter-agency counterterrorism efforts and, along with the FBI, has focused on ensuring that state and local law enforcement officials receive information on terrorist threats from national level intelligence agencies. [8, p. 3]

The Coast Guard, as part of DHS, deals with information relating to maritime security and homeland defense. The Energy Department analyzes foreign nuclear weapons programs as well as nuclear nonproliferation and energy-security issues. It also has a robust counterintelligence effort. The Treasury Department collects and processes information that may affect U.S. fiscal and monetary policies. Treasury also covers the terrorist financing issue. [8, p. 3]

The Intelligence Cycle

The Intelligence Cycle is the process of developing raw information into finished intelligence for use by policymakers, military commanders, and other consumers in decision making. This six-step cyclical process is highly dynamic, continuous, and never-ending. The sixth step, evaluation (which includes soliciting feedback from users) is conducted for each of the other five steps individually and for the Intelligence Cycle as a whole. [9, p. 10]

The Intelligence Cycle is the process of developing raw information into finished intelligence for use by policymakers, military commanders, and other consumers in decision making. This six-step cyclical process is highly dynamic, continuous, and never-ending.

Step 1: Planning and Direction. The planning and direction step sets the stage for the Intelligence Cycle. It is the springboard from which all Intelligence Cycle activities are launched. Oftentimes, the direction part of the step precedes the planning part. Generally, in such cases, the consumer has a requirement for a specific product. That product may be a full report, a graphic image, or raw information that is collected, processed, and disseminated, but skips the analysis and production step. Given the customer's requirement, the intelligence organization tasked with generating the product will then plan its Intelligence Cycle activities. [9, p. 11]

Step 2: Collection. Data collection is performed to gather raw data related to the five basic intelligence sources: 1) GEOINT, 2) HUMINT, 3) MASINT, 4) OSINT, and 5) SIGINT. The sources of the raw data may include, but are not limited to, news reports, aerial imagery, satellite imagery, and government and public documents. [9, p. 11]

Step 3: Processing and Exploitation. The processing and exploitation step (see the Glossary of Terms for a definition of "exploitation") involves the use of highly trained and specialized personnel and technologically sophisticated equipment to turn the raw data into usable and understandable information. Data translation, data decryption, and interpretation of filmed images and other imagery are only a few of the processes used for converting data stored on film, magnetic, or other media into information ready for analysis and production. [9, p. 11]

Step 4: Analysis and Production. The analysis and production step also requires highly trained and specialized personnel (in this case, analysts) to give meaning to the processed information and to prioritize it against known requirements. Synthesizing the processed information into a finished, actionable intelligence product enables the information to be useful to the customer. Note that, in some cases, the Intelligence Cycle may skip this step (for example, when the consumer needs only specific reported information or products such as raw imagery). This was the case during the Cuban Missile Crisis (October 1962) when President Kennedy needed only the actual number of pieces of Soviet equipment in Cuba and facts concerning reports on observed Soviet activity with no analysis of that information. [9, p. 12]

There are six basic intelligence sources, or collection disciplines:

1. *GEOINT*
2. *HUMINT*
3. *MASINT*
4. *OSINT*
5. *SIGINT*
6. *IMINT*

Step 5: Dissemination. The consumer that requested the information receives the finished product, usually via electronic transmission. Dissemination of the information typically is accomplished through such means as websites, email, Web 2.0 collaboration tools, and hardcopy distribution. The final, finished product is referred to as "finished intelligence." After the product is disseminated, further gaps in the intelligence may be identified, and the Intelligence Cycle begins all over again. [9, p. 12]

Step 6: Evaluation. Constant evaluation and feedback from consumers are extremely important to enabling those involved in the Intelligence Cycle to adjust and refine their activities and analysis to better meet consumers' changing and evolving information needs. [9, p. 12]

Intelligence Sources

There are six basic intelligence sources, or collection disciplines:

1. Geospatial Intelligence (GEOINT) is the exploitation and analysis of imagery, imagery intelligence (IMINT) (see the Glossary of Terms), and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. [9, p. 54]
2. Human Intelligence (HUMINT) is the collection of information—either orally or via documentation— that is provided directly by a human source. It is the only type of intelligence for which collectors speak directly to the sources of information, control the topic of discussion, and direct the source's activities. Human sources can obtain access to information that is not obtainable any other way. [9, pp. 53-54] The Director of the CIA serves as the National HUMINT Manager, but has delegated the day-to-day responsibilities of this position to the Director of the National Clandestine Service (D/NCS). [10]
3. Measurement and Signatures Intelligence (MASINT) is intelligence produced through quantitative and qualitative analysis of the physical attributes of targets and events to characterize and identify those targets and events. [9, p. 53]

Examples of this might be the distinctive radar signatures of specific aircraft systems or the chemical composition of air and water samples. The Directorate for MASINT and Technical Collection (DT), a component of the Defense Intelligence Agency, is the focus for all national and Department of Defense MASINT matters. [10]

4. Open-Source Intelligence (OSINT) is intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. [9, p. 54]
5. Signals Intelligence (SIGINT) is intelligence gathered from data transmissions, including Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT). SIGINT includes both raw data and the analysis of that data to produce intelligence. [9, p. 54] The National Security Agency is responsible for collecting, processing, and reporting SIGINT. The National SIGINT Committee within NSA advises the Director, NSA, and the DNI on SIGINT policy issues and manages the SIGINT requirements system. [10]
6. Imagery Intelligence (IMINT) includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, and electro -optics. The National Geospatial-Intelligence Agency is the manager for all imagery intelligence activities, both classified and unclassified, within the government, including requirements, collection, processing, exploitation, dissemination, archiving, and retrieval. [10]

Counterintelligence (CI) is the business of identifying and dealing with foreign intelligence threats to the United States and its interests.

Counterintelligence

Counterintelligence (CI) is the business of identifying and dealing with foreign intelligence threats to the United States and its interests. Its core concern is the intelligence services of foreign states and similar organizations of non-state actors, such as transnational terrorist groups. Counterintelligence has both a defensive mission - protecting the nation's secrets and assets against foreign intelligence penetration - and an offensive mission - finding out what foreign intelligence organizations are planning to better defeat their aims. [10]

As defined in Executive Order 12333 (and amended on 30 July 2008), "counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities." [10]

The Office of the National Counterintelligence Executive (ONCIX), under the leadership of the National Counterintelligence Executive (NCIX), was created to serve as the head of national counterintelligence for the USG and provide strategic direction to the counterintelligence community. [10]

ONCIX, through established programs, coordinates counterintelligence outreach efforts and the dissemination of warnings to the private sector on intelligence threats to the U.S. Visit the ONCIX website at www.ncix.gov for an in-depth look into the counterintelligence vision and mission for preserving our national security. [10]

In practice, U.S. law affords Fourth Amendment protection to all within the United States, citizen or not, and to all U.S. citizens everywhere, in the U.S. or not. Accordingly, "probable cause" must be demonstrated in order to obtain a warrant before conducting surveillance on somebody in the U.S., or a U.S. citizen abroad.

Domestic Surveillance

The Fourth Amendment to the U.S. Constitution guarantees "The right of people to be secure in their persons, house, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." In practice, U.S. law affords Fourth Amendment protection to all within the United States, citizen or not, and to all U.S. citizens everywhere, in the U.S. or not. Accordingly, "probable cause" must be demonstrated in order to obtain a warrant before conducting surveillance on somebody in the U.S., or a U.S. citizen abroad. For matters of national security, domestic surveillance warrants may be sought under provisions of the 1978 Foreign Intelligence Surveillance Act (FISA). [11]

In 2013, Edward Snowden, a former contractor employee working as a computer system administrator at an NSA facility in Hawaii, was charged with leaking top secret documents related to certain NSA programs to the Guardian and Washington Post newspapers. [12, p. 7]

The first program collected in bulk the phone records—including the number that was dialed from, the number that was dialed to, and the date and duration of the call—of customers of Verizon and possibly other U.S. telephone service providers. It did not collect the content of the calls or the identity of callers. The data was collected pursuant to Section 215 of the USA PATRIOT ACT, which amended the Foreign Intelligence Surveillance Act of 1978. Section 215 allowed the FBI, in this case on behalf of the NSA, to apply to the Foreign Intelligence Surveillance Court (FISC) for an order compelling a person to produce "any tangible thing," such as records held by a telecommunications provider, if the tangible things sought are "relevant to an authorized investigation." Some commentators expressed skepticism regarding how such a broad amount of data could be said to be "relevant to an authorized

investigation," as required by the statute. In response to these concerns, the Obama Administration subsequently declassified portions of the FISC order authorizing the program and issued a "whitepaper" describing the Administration's legal reasoning. [13, p. ii]

The second program, called PRISM, targeted the electronic communications, including content, of foreign targets overseas whose communications flow through American networks. These data were collected pursuant to Section 702 of FISA, which was added by the FISA Amendments Act of 2008. This program acquired information from Internet service providers, as well as through what NSA termed "upstream" collection that appeared to acquire Internet traffic while it was in transit from one location to another. Although the program targeted the communications of foreigners who were abroad, the Administration acknowledged that technical limitations in the "upstream" collection resulted in the collection of some communications that were unrelated to the target or that could take place between persons in the United States. Notwithstanding these technical limitations, the FISC held that this program was consistent with the requirements of both Section 702 and the Fourth Amendment provided that there were sufficient safeguards in place to identify and limit the retention, use, or dissemination of such unrelated or wholly domestic communications. [13, p. ii]

Following a contentious debate, the USA FREEDOM Act was finally passed and signed into law on June 2, 2015. Among its provisions, the USA FREEDOM Act restricted the use of FISA Section 215, effectively ending the NSA bulk collection programs.

The revelations prompted several lawsuits challenging the NSA programs. Congress also conducted hearings over their legitimacy. Following a contentious debate, the USA FREEDOM Act was finally passed and signed into law on June 2, 2015. Among its provisions, the USA FREEDOM Act restricted the use of FISA Section 215, effectively ending the NSA bulk collection programs. [14]

Conclusion

Since the 9/11 terrorist attacks, Congress has focused considerable attention on how intelligence is collected, analyzed, and disseminated in order to protect the homeland against terrorist threats. Prior to 9/11, it was possible to make a distinction between "domestic intelligence"—primarily law enforcement information collected within the United States—and "foreign intelligence"— primarily military, political, and economic intelligence collected outside the country. Today, threats to the homeland posed by terrorist groups are now national security threats. Intelligence collected outside the United States is often very relevant to the threat environment inside the United States and vice versa. [15, p. ii]

Challenge Your Understanding

The following questions are designed to challenge your understanding of the material presented in this chapter. Some questions may require additional research outside this book in order to provide a complete answer.

1. What is national intelligence?
2. Why was the CIA formed after World War II?
3. List and describe two high-profile intelligence failures over the last 30 years.
4. How did the 2004 Intelligence Reform Act enhance the authorities of the DNI compared to the DCI?
5. What is the purpose and function of the National Counterterrorism Center?
6. List and describe three different members of the Intelligence Community.
7. List and describe the six steps of the Intelligence cycle.
8. List and describe three different intelligence disciplines.
9. What is the necessary predicate to conduct surveillance of U.S. citizens?
10. Do you think Edward Snowden's actions were of benefit or harm to the nation? Explain your answer.

Chapter 38

Department of Defense

Learning Outcomes

Careful study of this chapter will help a student do the following:

- Explain the difference between active and reserve military forces.
- Describe the unique capabilities of the National Guard.
- Discuss the homeland defense mission.
- Discuss defense support of civil authorities.
- Explain the purpose and authority of a dual-status commander.
- Identify unique roles and responsibilities of USNORTHCOM.