CHAPTER SIX

PREDICTION AND PREVENTION

The Role of Intelligence

Opening Viewpoint: Prevention: A Case of Successful International Intelligence Cooperation

An example of successful international intelligence cooperation occurred in May 2002 between American and Moroccan intelligence agencies. In February 2002, Moroccan intelligence officers interrogated Moroccan al-Qaeda prisoners held by the Americans at their naval base in Guantánamo Bay, Cuba. They received information from one of the prisoners about an al-Qaeda operative in Morocco and also received information about the operative's relatives. Moroccan officials obtained a sketched description of the man from the relatives and showed the sketch to the Guantánamo prisoner, who confirmed his likeness. The Moroccans located the suspect (a Saudi), followed him for a month, and eventually arrested him and two Saudi accomplices. The suspects eventually told the Moroccans that they were al-Qaeda operatives trained in Afghanistan and that they had escaped during the anti-Taliban campaign after receiving orders to engage in suicide attacks against maritime targets in Gibraltar. They had begun the process of inquiring about speedboats, and their ultimate targets were to be U.S. Navy ships passing through Gibraltar.

Chapter Learning Objectives

This chapter will enable readers to do the following:

1. Analyze challenges inherent in the mission of the Intelligence Community
2. Understand the organizational alignments of the Intelligence Community
3. Evaluate the types of intelligence and how intelligence is collected
4. Apply the role of intelligence collection to the context of the homeland security enterprise
5. Remember the missions of intelligence agencies
6. Understand the complexity of the intelligence craft and the roles of intelligence agencies

Intelligence refers to the collection of data. Its purpose within the context of counterterrorism is to create an informational database about terrorist movements and predict terrorist behavior. This process is not unlike that of criminal justice investigators who work to resolve criminal cases. In both contexts, the fundamental objectives of intelligence collection are prediction and prevention.

Intelligence Community: The greater network of intelligence agencies. In the United States, the Central Intelligence Agency is the theoretical coordinator of intelligence collection.

The modern **Intelligence Community** (IC) comprises mission-specific agencies representing the predictive and analytical arm of the federal government. It manages the collection and analysis of an enormous quantity of information derived from an extremely diverse array of sources. The Intelligence Community must filter this information in order to create actionable intelligence, which is critically necessary for predicting, preventing, and analyzing terrorist events. Intelligence agencies involve themselves with the collection and analysis of information. The underlying mission of intelligence agencies is to construct an accurate activity profile of terrorists. Data are collected from overt and covert sources and evaluated by expert intelligence analysts. This process—intelligence collection and analysis—is at the heart of the counterterrorist intelligence mission.

The outcome of high-quality intelligence collection and analysis can range from the construction of profiles of terrorist organizations to tracking the movements of terrorists. An optimal outcome of counterterrorist intelligence is the ability to *anticipate* the behavior of terrorists and thereby to predict terrorist incidents. However, exact prediction is relatively rare, and most intelligence on terrorist threats is generalized rather than specific. For example, intelligence agencies have had success in uncovering threats in specific cities by specific groups but less success in predicting the exact time and place of possible attacks. These considerations are summarized as elements of the overall mission of the IC:

> The Intelligence Community's mission is to collect, analyse, and deliver foreign intelligence and counterterrorist information to America's leaders so they can make sound decisions to protect our country.[1]

The discussion in this chapter addresses the role of intelligence and the mission of the Intelligence Community. Inherent in this discussion is the tension that naturally arises between the mission of the IC and the challenges of intelligence coordination, collection, and analysis. This chapter examines the following issues:

- The U.S. Intelligence Community: Mission
- The intelligence cycle
- Intelligence oversight
- Intelligence agencies
- The U.S. Intelligence Community: Challenges

THE U.S. INTELLIGENCE COMMUNITY: MISSION

Intelligence collection and analysis are important components of the homeland security enterprise. The intelligence mission is unique in the sense that it is responsible for securing the American homeland from external threats. That is, although intelligence operations have a significant effect on domestic security, their scope of operations is also outside the borders of the nation.

Background: Intelligence Collection and Jurisdiction

Federal National Security Intelligence Collection

National security intelligence collection is divided between agencies that are separately responsible for domestic and international intelligence collection. This separation is

mandated by law. For example, the **Federal Bureau of Investigation (FBI)** performs domestic intelligence collection, and the **Central Intelligence Agency (CIA)** operates internationally. The FBI is a law enforcement agency that uses criminal intelligence to enforce the law and provides important assistance to state and local law enforcement agencies. However, the FBI also has primary jurisdiction over domestic counterintelligence and counterterrorist surveillance and investigations. The CIA is not a law enforcement agency and, therefore, officially performs a supportive role in domestic counterterrorist investigations.

Other federal agencies, such as the **Diplomatic Security Service**, also assist in tracking suspects wanted for acts of terrorism. The Diplomatic Security Service is a security bureau within the U.S. Department of State that, among other duties, manages an international bounty program called the **Rewards for Justice Program**. The program offers cash rewards for information leading to the arrest of wanted terrorists. The Rewards for Justice Program has successfully resulted in the capture of suspects.

Central Intelligence Agency (CIA): The principal intelligence agency in the United States and the theoretical coordinator of American foreign intelligence collection.

Diplomatic Security Service: A security bureau within the U.S. Department of State that protects diplomats and other officials.

Rewards for Justice Program: An international bounty program managed by the U.S. Diplomatic Security Service. The program offers cash rewards for information leading to the arrest of wanted terrorists.

State and Local Intelligence Collection

State and local intelligence collection has its origin in crime prevention and prediction. Law enforcement agencies have a long history of building criminal intelligence databases for the purpose of preventing and predicting criminal activity, and these databases are readily adaptable to providing information relevant to the national security mission of the homeland security enterprise. Modern databases are frequently linked to the FBI's criminal and forensic databases, thus creating an intertwined system of intelligence-sharing and -tracking capability. Collaborative networks and initiatives have been established to promote collaboration on intelligence sharing. Examples of these networks and initiatives include the following:

- *Homeland Security Information Network (HSIN)*. "The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive But Unclassified information. . . . The Homeland Security Information Network (HSIN) provides law enforcement officials at every level of government with a means to collaborate securely with partners across geographic and jurisdictional boundaries."[2]
- *National Criminal Intelligence Sharing Plan (NCISP)*. Developed in 2003, "this plan represents law enforcement's commitment to take it upon itself to ensure that the dots are connected, be it in crime or terrorism. The plan is the outcome of an unprecedented effort by law enforcement agencies, with the strong support of the Department of Justice, to strengthen the nation's security through better intelligence analysis and sharing."[3]
- *Regional Information Sharing System (RISS)*. Created in 1973, RISS "offers secure information sharing and communications capabilities, critical analytical and investigative support services, and event deconfliction to enhance officer safety. RISS supports efforts against organized and violent crime, gang activity, drug activity, terrorism, human trafficking, identity theft, and other regional priorities."[4]

Evolution of the Modern Intelligence Community

The present-day IC is a successor to the missions and organizational configurations that were established during the Cold War. Rivalry between the United States and the Soviet Union, and their respective "Free World" and "Eastern Bloc" allies, necessitated the creation and funding of a global intelligence presence. At its peak during the 1980s, the IC employed

approximately 100,000 personnel. The IC workforce was assigned to approximately 25 agencies and elements. Each organization was tasked with performing specialized functions, often using assigned modalities of intelligence collection such as electronic surveillance or the deployment of human assets. Expansion of the Cold War–era IC necessitated a concomitant increase of fiscal resources, eventually resulting in the appropriation of approximately $30 billion for IC operations. With the end of the Cold War—dated roughly from the 1989 dismantling of the Berlin Wall—there occurred a consolidation process of hitherto discrete agency operations. Fiscal appropriations were reduced, as were the number of IC personnel, agencies, and elements.

With the post–Cold War reductions in appropriations and personnel, the IC directed much of its attention toward counterterrorist operations. This was a matter of necessity because of the following incidents:

- 1993: Vehicular bombing of the World Trade Center in New York City by Ramzi Yousef.
- 1998: Simultaneous suicide bombings of the American embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, by al-Qaeda operatives.
- 2000: Suicide attack on the destroyer USS *Cole* in Aden, Yemen.

These and other incidents indicated that determined terrorists have the ability to carry out significant attacks despite the hard work of the U.S. IC and allied intelligence agencies. The successful al-Qaeda attacks on September 11, 2001, led to the creation in November 2002 of the National Commission on Terrorist Attacks Upon the United States. Established jointly by law by Congress and President George W. Bush, it is commonly referred to as the *9/11 Commission*. The 9/11 Commission was a bipartisan panel directed to

> investigate "facts and circumstances relating to the terrorist attacks of September 11, 2001," including those relating to intelligence agencies, law enforcement agencies, diplomacy, immigration issues and border control. The flow of assets to terrorist organizations, commercial aviation, the role of congressional oversight and resource allocation, and other areas determined relevant by the Commission.[5]

The final chapter of the 9/11 Commission's report is titled "How to Do It? A Different Way of Organizing the Government." In this chapter, the 9/11 Commission stressed the need for unity of effort and specifically provided detailed and pointed recommendations for restructuring the IC. It stated that "[t]he need to restructure the Intelligence Community grows out of six problems that have become apparent before and after 9/11:

- "*Structural barriers to performing joint intelligence work*. National intelligence is still organized around the collection disciplines of the home agencies, not the joint mission. The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to 'connect the dots.' No one component holds all the relevant information.
- "*Lack of common standards and practices across the foreign-domestic divide*. The leadership of the Intelligence Community should be able to pool information gathered overseas with information gathered in the United States, holding the work—wherever it is done—to a common standard of quality in how it is collected, processed (e.g., translated), reported,

shared, and analyzed. A common set of personnel standards for intelligence can create a group of professionals better able to operate in joint activities, transcending their own service-specific mind-sets.

- "*Divided management of national intelligence capabilities*. While the CIA was once "central" to our national intelligence capabilities, following the end of the Cold War it has been less able to influence the use of the nation's imagery and signals intelligence capabilities in three national agencies housed within the Department of Defense: the National Security Agency, the National Geospatial-Intelligence Agency, and the National Reconnaissance Office. One of the lessons learned from the 1991 Gulf War was the value of national intelligence systems (satellites in particular) in precision warfare. Since that war, the department has appropriately drawn these agencies into its transformation of the military. Helping to orchestrate this transformation is the Under Secretary of Defense for Intelligence, a position established by Congress after 9/11. An unintended consequence of these developments has been the far greater demand made by Defense on technical systems, leaving the Director of Central Intelligence (DCI) less able to influence how these technical resources are allocated and used.

- "*Weak capacity to set priorities and move resources*. The agencies are mainly organized around what they collect or the way they collect it. But the priorities for collection are national. As the DCI makes hard choices about moving resources, he or she must have the power to reach across agencies and reallocate effort.

- "*Too many jobs*. The DCI now has at least three jobs. He is expected to run a particular agency, the CIA. He is expected to manage the loose confederation of agencies that is the Intelligence Community. He is expected to be the analyst in chief for the government, sifting evidence and directly briefing the President as his principal intelligence adviser. No recent DCI has been able to do all three effectively. Usually what loses out is management of the Intelligence Community, a difficult task even in the best case because the DCI's current authorities are weak. With so much to do, the DCI often has not used even the authority he has.

- "*Too complex and secret*. Over the decades, the agencies and the rules surrounding the Intelligence Community have accumulated to a depth that practically defies public comprehension. There are now 15 agencies or parts of agencies in the Intelligence Community. The community and the DCI's authorities have become arcane matters, understood only by initiates after long study. Even the most basic information about how much money is actually allocated to or within the Intelligence Community and most of its key components is shrouded from public view."[6]

In recognition of the 9/11 Commission's conclusions, and to reduce the incidence of problems cited by the Commission, in December 2004, the IC was reorganized with the passage of the Intelligence Reform and Terrorism Prevention Act (IRTA). Of central importance to the IC reorganization was the creation of two new elements, the **Office of the Director of National Intelligence (ODNI)** and the **National Counterterrorism Center (NCTC)**. Members of the community were subsumed under the direction of the new ODNI. President George W. Bush appointed John Negroponte, former U.S. ambassador to Iraq, as the United States' first **Director of National Intelligence** (DNI). Officially confirmed by the Senate in April 2005, the DNI is responsible for coordinating the various components of the IC.

Office of the Director of National Intelligence (ODNI): In December 2004, the intelligence community was reorganized with the passage of the Intelligence Reform and Terrorism Prevention Act. Members of the community were subsumed under the direction of a new Office of the Director of National Intelligence, responsible for coordinating the various components of the intelligence community.

National Counterterrorism Center (NCTC): A center established to integrate the counterterrorism efforts of the intelligence community in the wake of the September 11, 2001, attacks.

Director of National Intelligence: Members of the IC are subsumed under the direction of the ODNI. President George W. Bush appointed John Negroponte, former U.S. ambassador to Iraq, as the United States' first Director of National Intelligence (DNI). The DNI is responsible for coordinating the various components of the IC.

Thus, in the post–9/11 era, the United States endeavors to advance the quality of intelligence collection and analysis by creating a coordinated and cooperative IC. This philosophy of collaboration is the primary conceptual goal of the American counterterrorist intelligence effort.

The Intelligence Community in the Post–9/11 Environment

The modern IC is comprised of agencies that function under the authority of the executive branch of government. They are administratively independent agencies that ideally cooperate in the collection and analysis of information. All agencies are tasked with providing information to the president and other relevant stakeholders on a "need to know" basis. The IC is an extensive administrative enterprise consisting of 17 elements—16 agencies and the ODNI—organized as follows:

- Office of the Director of National Intelligence
- Central Intelligence Agency
- National Security Agency
- Federal Bureau of Investigation
- Department of State (Bureau of Intelligence and Research)
- Department of Energy (Office of Intelligence and Counterintelligence)
- Drug Enforcement Administration (Office of National Security Intelligence)
- Department of Homeland Security (Office of Intelligence and Analysis)
- Department of Treasury (Office of Intelligence and Analysis)
- Defense Intelligence Agency
- Office of Naval Intelligence
- Army Intelligence and Security Command
- Marine Corps Intelligence
- Air Force Intelligence
- U.S. Coast Guard Intelligence
- National Reconnaissance Office
- National Geospatial-Intelligence Agency

Each agency must comply with mandated jurisdictional limitations on its collection of intelligence. However, because national security threats may affect multiple sectors of the homeland security enterprise, there naturally exists overlap in jurisdiction among some agencies. For example, the following problems may involve complex scenarios that activate the jurisdiction of multiple agencies:

- Threats from violent extremists
- Countering foreign intelligence operations in the United States
- Illicit weapons trafficking

- Drug trafficking
- Human trafficking
- Cyberattacks
- CBRN (chemical, biological, radiological, nuclear) threats
- Threats against infrastructure

Because of the segmentation of the IC and the complexity of its overall mission, there exists an imperative need for seamless coordination and cooperation among organizations comprising the IC. As discussed later in this chapter, the ideal of interagency collaboration is sometimes a challenging goal. Nevertheless, because of the critical need for actionable information, the IC is a central component of the homeland security enterprise.

THE INTELLIGENCE CYCLE

The Intelligence Community operates within the framework of an intelligence cycle. Ideally, the intelligence cycle represents a seamless and efficient process for providing accurate information to policymakers, who use intelligence findings to design and implement informed policies. Agencies comprising the IC are tasked to select methods for collecting desired information and to operationalize these methods. When information is successfully obtained, specialists organize, interpret, and analyze the significance of their findings. This is a dynamic process that frequently engenders new questions and new intelligence operations.

Phases of the Intelligence Cycle

The intelligence cycle involves six phases. These phases are often compartmentalized processes, consisting of the following components:

- *Planning and Direction:* "Policymakers—including the president, presidential advisors, the National Security Council, and other major departments and agencies—determine what issues need to be addressed and set intelligence priorities. The IC's issue coordinators interact with these officials to identify core concerns and information requirements."[7]
- *Collection:* "The IC uses many methods to collect information, including face-to-face meetings with human sources, technical and physical surveillance, satellite surveillance, interviews, searches, and liaison relationships. Information can be gathered through open, covert, and electronic means. All collection methods must be lawful and are subject to oversight by Congress and others. Information collected must be relevant, timely, and useful. At this state, the information is often referred to as raw intelligence, because it hasn't been thoroughly examined and evaluated yet."[8]
- *Processing:* "The collection stage of the intelligence cycle can yield large amounts of data that requires organization and refinement. Substantial resources are devoted to synthesizing this data into a form that intelligence analysts can use."[9]
- *Analysis and Production:* "Analysts examine and evaluate all the information collected, add context as needed, and integrate it into complete products. They produce *finished intelligence* that includes assessments of events and judgments about the implications of the information for the United States."[10]

- *Dissemination:* "Finished intelligence is delivered to policymakers, military leaders, and other senior government leaders who then make decisions based on the information. Finished intelligence can lead to requests for additional information, thus triggering the intelligence cycle again."[11]
- *Evaluation:* Although this is listed as a discrete step in the intelligence cycle, evaluation . . . is ongoing throughout the cycle. [The IC is] continuously evaluating . . . products for relevance, bias, accuracy, and timeliness, as well as [the] process to ensure it is efficient and thorough."[12]

Types of Intelligence Collection

signals intelligence (SIGINT): Intelligence that has been collected by technological resources.

human intelligence (HUMINT): Intelligence that has been collected by human operatives rather than through technological resources.

open source intelligence (OSINT): Information collected from publicly available electronic and print outlets. It is information that is readily available to the public, but used for intelligence analysis. Examples of open sources include newspapers, the Internet, journals, radio, videos, television, and commercial outlets.

imagery intelligence (IMINT): Images are regularly collected to provide actionable intelligence. Collection technologies range from relatively routine hand-held equipment to very sophisticated means. IMINT includes intelligence information derived from the collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors.

The cycle of intelligence collection requires the marshaling of an integrated system of technologies, specialized agencies, professional practitioners, and collaborative government entities. This is often a complex endeavor. Nevertheless, the following six source types are routinely deployed from the IC:

SIGINT—Signal Intelligence

Intelligence collection and analysis in the modern era require the use of sophisticated technological resources. These technological resources are used primarily for the interception of electronic signals—known as **signals intelligence (SIGINT)**. SIGINT is used for a variety of purposes, such as interceptions of financial data, monitoring communications such as cell phone conversations, and reading e-mail messages. The use of satellite imagery is also commonly used by intelligence agencies, and sophisticated computers specialize in code breaking. However, the practicality of these technologies as counterterrorist options is limited in the era of the New Terrorism. Because of the cellular organizational structure of terrorist groups and their insular interactions (i.e., based on personal relationships), technology cannot be an exclusive counterterrorist resource. Human intelligence is also a critical component. Prominent SIGINT centers include the United Kingdom's Government Communications Headquarters (GCHQ) and the National Security Agency (NSA) in the United States.

HUMINT—Human Intelligence

The collection of **human intelligence**, also referred to as **HUMINT**, is often a cooperative venture with friendly intelligence agencies and law enforcement officials. This sharing of information is a critical component of counterterrorist intelligence gathering. Circumstances may also require the covert manipulation of individuals affiliated with terrorist organizations or their support groups, with the objective of convincing them to become intelligence agents. The manipulation process can include making appeals to potential spies' sense of justice or patriotism, paying them with money and other valuables, or offering them something that they would otherwise be unable to obtain (such as asylum for their family in a Western country). One significant problem with finding resources for human intelligence is that most terrorist cells are made up of individuals who know one another very well. Newcomers are not openly welcomed, and those who may be potential members are usually expected to commit an act of terrorism or other crime to prove their commitment to the cause. In other words, intelligence agencies must be willing to use terrorists to catch terrorists. This has been a very difficult task, and groups such as al-Qaeda have proven very difficult to penetrate with human assets.[13]

OSINT—Open Source Intelligence

Open source intelligence (OSINT) is information collected from publicly available electronic and print outlets. It is information that is readily available to the public but used for intelligence analysis. Examples of open sources include newspapers, the Internet, journals, radio, videos, television, and commercial outlets.

IMINT—Imagery Intelligence

Images are regularly collected to provide actionable intelligence. Collection technologies range from relatively routine hand-held equipment to very sophisticated means. **Imagery intelligence (IMINT)** includes "intelligence information derived from the collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors."[14]

MASINT—Measurements and Signatures Intelligence

The use of a broad array of technical and scientific disciplines to measure the characteristics of specified subjects—for example, tracking communications signatures or measuring water and soil samples. **Measurements and signatures intelligence (MASINT)** is "intelligence information obtained by quantitative and qualitative analysis of data derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender."[15]

GEOINT—Geospatial Intelligence

The collection and assessment of topography and geographical features can provide actionable intelligence regarding locations, timeframes, and other information. **Geospatial intelligence (GEOINT)** is "the all-source analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on earth."[16]

The National Intelligence Priorities Framework

Intelligence policy priorities are governed by the **National Intelligence Priorities Framework** (NIPF), which "promulgates policy and establishes responsibilities for setting national intelligence priorities and translating them into action."[17]

The Director of National Intelligence is charged with overall authority to assure compliance with NIPF guidelines and is required to "approve the NIPF and the policies and processes for establishing national intelligence priorities; and adjust national intelligence priorities as necessary."[18]

This is done under consideration from, and on the recommendation of, heads of agencies that comprise the IC. It is necessary to regularly update the NIPF. Updates are intended to provide fresh direction for intelligence agencies on how best to allocate resources for intelligence collection and analysis. In theory, it is a process that promotes efficiency within the IC.

measurements and signatures intelligence (MASINT): The use of a broad array of technical and scientific disciplines to measure the characteristics of specified subjects. For example, tracking communications signatures or measuring water and soil samples. MASINT is intelligence information obtained by quantitative and qualitative analysis of data derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender.

geospatial intelligence (GEOINT): The collection and assessment of topography and geographical features can provide actionable intelligence regarding locations, timeframes, and other information. GEOINT is the all-source analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on earth.

National Intelligence Priorities Framework: Intelligence policy priorities are governed by the National Intelligence Priorities Framework (NIPF), which promulgates policy and establishes responsibilities for setting national intelligence priorities and translating them into action.

INTELLIGENCE OVERSIGHT

The Intelligence Community technically operates under the purview of the executive branch of government. However, because the work of the IC is quite often highly sensitive with potentially significant ramifications, the IC also operates under the oversight of several

federal policy centers. These oversight centers are drawn from the executive, legislative, and judiciary branches of government. The purpose of intelligence oversight is to confirm that the work of the IC is in compliance with relevant laws and policies. Offices possessing oversight authority within the executive branch include

- the office of the President,
- the National Security Council,
- the President's Intelligence Advisory Board,
- the Intelligence Oversight Board,
- the Office of Management and Budget, and
- the Privacy and Civil Liberties Oversight Board.

Offices possessing oversight authority within the legislative branch include

- the Senate Select Committee on Intelligence and
- the House Permanent Select Committee on Intelligence.

The Foreign Intelligence Surveillance Court is also authorized to provide oversight from within the judiciary branch. Additional oversight may originate from inspectors general operating from within each IC agency. Inspectors general conduct audits and other reviews of IC agencies.

INTELLIGENCE AGENCIES

Members of the American Intelligence Community include the following agencies and centers.

Office of the Director of National Intelligence

The ODNI was created to address concerns about the efficiency of the IC in the aftermath of the attacks on September 11, 2001. As stated on the office's website, "the mission of the ODNI is to lead and support IC integration; delivering insights, driving capabilities, and investing in the future."[19] Furthermore, "The ODNI is staffed by officers from across the IC and is organized into directorates, centers, and oversight offices that support the DNI's role as head of the IC and manager of the National Intelligence Program (NIP)."[20]

ODNI directorates "are organized around ODNI core functions to provide a more holistic view and strategic approach to intelligence integration."[21] Established directorates include Enterprise Capacity, Mission Integration, National Security Partnerships, and Strategy and Engagement.

ODNI mission centers include the Cyber Threat Integration Center, National Counterproliferation Center, National Counterintelligence and Security Center, and the National Counterterrorism Center. The mission centers perform critical tasks for the homeland security enterprise. As explained by the ODNI,

> In their roles as functional National Intelligence Managers (NIMs), the National Counterterrorism Center (NCTC), the National Counterproliferation Center (NCPC), and the National Counterintelligence and Security Center (NCSC)

also contribute to the mission of intelligence integration. For both functional and regional NIMs, the Unifying Intelligence Strategies (UIS) are critical plans for communicating priorities and achieving intelligence integration. NIMs develop UIS in line with prioritized IC requirements and are charged with leading integration across the IC by function and region.[22]

ODNI oversight offices include Civil Liberties, Privacy and Transparency; Equal Employment Opportunity and Diversity; Intelligence Community Inspector General; and Office of General Counsel. These offices function as internal controls to

> ensure that the IC carries out its mission in a manner that protects privacy and civil liberties and enhances transparency; oversee equal opportunity and workforce diversity programs; conduct independent audits, investigations, inspections, and reviews; provide accurate legal guidance and counsel to ensure compliance with the Constitution, U.S. law, and corresponding regulations; and facilitate the DNI's statutory responsibility to keep the appropriate Congressional committees informed of all intelligence activities of the U.S.[23]

National Security Agency (NSA): An American intelligence agency charged with signals intelligence collection, code making, and code breaking.

National Security Agency

The **National Security Agency (NSA)** is the technological arm of the U.S. Intelligence Community. Using state-of-the-art computer and satellite technologies, the NSA's primary mission is to collect communications and other signal intelligence. It also devotes a significant portion of its technological expertise to code-making and code-breaking activities. Much of this work is done covertly from secret surveillance facilities positioned around the globe.

Central Intelligence Agency

The CIA is an independent federal agency. It is the theoretical coordinator of the Intelligence Community. The agency is charged with collecting intelligence outside of the borders of the United States, which is done covertly using human and technological assets. The CIA is legally prohibited from collecting intelligence inside the United States.

U.S. National Security Agency

▸ Photo 6.1

Defense Intelligence Agency

The **Defense Intelligence Agency (DIA)** is a bureau within the Department of Defense. It is the central intelligence bureau for the U.S. military. Each branch of the military coordinates its intelligence collection and analysis with the other branches through the DIA.

Defense Intelligence Agency (DIA): The central agency for military intelligence of the U.S. armed forces.

Federal Bureau of Investigation

The FBI is a bureau within the Department of Justice. It is a law enforcement agency that is charged, in part, with conducting domestic surveillance of suspected spies and terrorists. The agency also engages in domestic intelligence collection and has been deployed to American embassies around the world. Foreign counterintelligence investigations have included an FBI presence at the sites of the 1998 bombings of the U.S. embassies in Kenya and Tanzania.

U.S. National Security Agency

▸ Photo 6.2

National Geospatial-Intelligence Agency

The **National Geospatial-Intelligence Agency (NGA)** is responsible for overseeing GEOINT collection and analysis. NGA "manages a global consortium of more than 400 commercial and government relationships." Furthermore, "[t]he director of NGA serves as the functional manager for GEOINT, the head of the National System for Geospatial Intelligence and the coordinator of the global Allied System for Geospatial Intelligence."[24]

National Reconnaissance Office

The **National Reconnaissance Office** (NRO) is responsible for "designing, building, launching, and maintaining America's intelligence satellites."[25] NRO provides satellite reconnaissance support to the IC and Department of Defense.

National Reconnaissance Office: Responsible for designing, building, launching, and maintaining America's intelligence satellites. NRO provides satellite reconnaissance support to the IC and Department of Defense.

Department of Homeland Security Office of Intelligence and Analysis

The **DHS Office of Intelligence and Analysis** (I&A) is a unique member of the IC. Unlike other agencies, "I&A is the only Intelligence Community (IC) element statutorily charged with delivering intelligence to our state, local, tribal, territorial, and private-sector partners, and developing intelligence from those partners for [DHS] and the IC."[26]

DHS Office of Intelligence and Analysis: The only Intelligence Community (IC) element statutorily charged with delivering intelligence to state, local, tribal, territorial, and private-sector partners, and developing intelligence from those partners for [DHS] and the IC.

Case in Point: The International Context of Intelligence

In many democracies, intelligence collection is traditionally divided between agencies that are separately responsible for domestic and international intelligence collection. This separation is often mandated by law. For example, the following agencies roughly parallel one another's missions:

- In Great Britain, the Security Service (**MI5**) is responsible for domestic intelligence, and the Secret Intelligence Service (**MI6**) is responsible for international collection. GCHQ provides SIGINT support for both MI5 and MI6.
- In Germany, the **Bureau for the Protection of the Constitution** shares a mission similar to MI5 and the FBI, and the **Military Intelligence Service** roughly parallels MI6 and the CIA. SIGINT support is provided by several centers, including the Military Intelligence Service and the Bundeswehr's (united armed forces) Strategic Reconnaissance Command.

THE U.S. INTELLIGENCE COMMUNITY: CHALLENGES

The collection and analysis of intelligence are covert processes that do not lend themselves easily to absolute cooperation and coordination between countries or between members of domestic intelligence communities. National intelligence agencies do not readily share intelligence with allied countries; they usually do so only after careful deliberation. The same is true of intelligence communities within countries. For example, prior to the September 11, 2001, homeland attacks, dozens of federal agencies were involved in the collection of

intelligence about terrorism. This led to overlapping and competing interests. A case in point is the apparent failure by the FBI and CIA to collaboratively process, share, and evaluate important intelligence between their agencies. In the case of the FBI, there was also an apparent failure of coordination between the agency's field and national offices. These problems precipitated a proposal in June 2002 by President Bush to completely reorganize the American homeland security community.

Problems of Collection and Analysis

Intelligence collection and analysis are not always exact or low-risk sciences. They can reflect only the quality and amount of data that are available. Because of the nature of counterterrorist intelligence collection and analysis, some experts in the United States have concluded that "the inherent difficulties in both collection and analysis of intelligence on terrorism mean that there will never be tactical warning of most attempted terrorist attacks, or even most major attempted attacks against U.S. targets."[27]

This observation became controversially apparent on July 7, 2004, when the U.S. Select Committee on Intelligence issued its extensive *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*.[28] The 521-page report's findings were a scathing critique of intelligence failures regarding Iraq. For example, its first conclusion found the following:

> Most of the major key judgments in the Intelligence Community's October 2002 National Intelligence Estimate (NIE), *Iraq's Continuing Programs for Weapons of Mass Destruction*, either overstated, or were not supported by, the underlying intelligence reporting. A series of failures, particularly in analytic trade craft, led to mischaracterization of the intelligence.[29]

In another highly critical report, a presidential commission known as the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction essentially labeled the American Intelligence Community as being dysfunctional.[30] It also said that the causes for the failure in the Iraq case continued to hinder intelligence on other potential threats, such as the nuclear programs of adversaries. The commission's 601-page report was delivered in March 2005.

Interagency Coordination and Cooperation

Among law enforcement agencies, the FBI is one of the few agencies that performs a quasi-security mission, explicitly adopting as one of its primary missions the protection of the United States from foreign intelligence and terrorist threats. The FBI does this through one of its five functional areas, the Foreign Counterintelligence functional area. The FBI also maintains missions in several U.S. embassies to coordinate its investigations of cases with international links. Among the service agencies, several bureaus perform a variety of security missions. For example, the Secret Service (part of the Department of the Treasury) protects the president, and the Federal Emergency Management Agency responds to natural and human-made disasters.

An ideal policy framework would require the FBI and CIA to coordinate and share counterterrorist intelligence in a spirit of absolute cooperation. In theory, the FBI should focus on investigating possible domestic security threats, and the CIA should pass along foreign intelligence that might affect domestic security.

Prior to the September 11, 2001, organizational crisis, homeland security was the responsibility of a number of federal agencies. These agencies were not centrally coordinated,

and they answered to different centers of authority. Cooperation was theoretically ensured by liaison protocols, special task forces, and oversight. In reality, there was a great deal of functional overlap and bureaucratic "turf" issues.

One problem that became quite clear during the year following the September 11, 2001, homeland attacks was that the pre–9/11 organizational model did not adapt well to the new security crisis. This failure to adapt proved to be operationally damaging; it was politically embarrassing, and it projected an image of disarray.

Intelligence Transformation After September 11, 2001

Consolidation of the domestic security community into an efficient homeland security enterprise became a critical priority in the aftermath of the September 11 attacks. Two efforts were given particular priority: transformation of the Intelligence Community and creation of a new homeland security institutional culture.

A series of revelations and allegations called into question previous assertions by the FBI and CIA that neither agency had prior intelligence about the September 11 homeland attacks. For example, it was discovered that

- the FBI had been aware for years prior to September 2001 that foreign nationals were enrolling in flight schools, and
- the CIA had compiled intelligence data about some members of the al-Qaeda cell that carried out the attacks.

These allegations were compounded by a leak to the press of a memorandum from an FBI field agent that strongly condemned the FBI director's and headquarters' handling of field intelligence reports about Zacarias Moussaoui. Moussaoui was alleged to have been a member of the September 11, 2001, al-Qaeda cell; he had been jailed prior to the attacks. Moussaoui had tried to enroll in flying classes, in which he was apparently interested only in how to *fly* airplanes and uninterested in the *landing* portion of the classes.

Policymakers and elected leaders wanted to know why neither the FBI nor the CIA had "connected the dots" to create a single intelligence profile. Serious interagency and internal problems became publicly apparent when a cycle of recriminations, press leaks, and congressional interventions damaged the "united front" image projected by the White House. Policymakers determined that problems in the homeland security community included the following:

- Long-standing interagency rivalries
- Entrenched and cumbersome bureaucratic cultures and procedures
- No central coordination of homeland security programs
- Fragmentation of counterterrorist operations
- Poor coordination of counterterrorist intelligence collection and analysis
- Disconnect between field offices and Washington headquarters
- "Turf"-based conflict between the FBI and CIA

Subsequent commission reports led to sweeping changes in the U.S. Intelligence Community. These reports included the following:

- In July 2004, the 9/11 Commission issued its detailed report on the September 11, 2001, attacks.
- In March 2005, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction issued its detailed report on intelligence failures regarding the possession and proliferation of weapons of mass destruction.

The **National Counterterrorism Center (NCTC)** was established to integrate the counterterrorism efforts of the Intelligence Community. Although some jurisdictional tension existed between the NCTC and the CIA's Counterterrorism Center, the NCTC became an important component of the new homeland security culture in the United States. Clearly, the attacks of September 11, 2001, were the catalyst for a broad and long-standing reconfiguration of the American security environment.[31]

Homeland security's counterterrorist bureaucracy is conceptually an amalgamation of many functions of law enforcement and intelligence agencies as well as branches of the military. The bureaucratic ideal of rationality and efficiency requires that these sectors of the government coordinate their counterterrorist missions to promote homeland security. For example, domestic law enforcement agencies must be kept apprised of terrorist threats that may be discovered abroad by intelligence agencies or the military—the challenge is how to implement this policy in these and other scenarios.

Case in Point: Intelligence Miscalculation and the Iraq Case

One of the most disturbing scenarios involved the delivery of weapons of mass destruction (WMDs) to motivated terrorists by an aggressive authoritarian regime. This scenario was the underlying rationale given for the March 2003 invasion of Iraq by the United States and several allies.

In January 2002, U.S. president George W. Bush identified Iraq, Iran, and North Korea as the "axis of evil" and promised that the United States "will not permit the world's most dangerous regimes to threaten us with the world's most destructive weapons." In June 2002, President Bush announced during a speech at the U.S. Military Academy at West Point that the United States would engage in preemptive warfare if necessary.

Citing Iraq's known possession of weapons of mass destruction in the recent past and its alleged ties to international terrorist networks, President Bush informed the United Nations (UN) in September 2002 that the United States would unilaterally move against Iraq if the UN did not certify that Iraq no longer possessed WMDs. Congress authorized an attack on Iraq in October 2002. UN weapons inspectors returned to Iraq in November 2002. After a three-month military buildup, Iraq was attacked on March 20, 2003, and Baghdad fell to U.S. troops on April 9, 2003.

The Bush administration had repeatedly argued that Iraq still possessed a significant arsenal of WMDs at the time of the invasion, that Hussein's regime had close ties to terrorist groups, and that a preemptive war was necessary to prevent the delivery of these weapons to al-Qaeda or another network. Although many experts discounted links between Hussein's regime and religious terrorists, it was widely expected that WMDs would be found. Iraq was known to have used chemical weapons against Iranian troops during the Iran-Iraq War of 1980–1988 and against Iraqi Kurds during the Anfal Campaign of 1987.

In actuality, UN inspectors identified no WMDs prior to the 2003 invasion, nor were WMDs found by U.S. officials during the occupation of Iraq. Also, little evidence was uncovered to substantiate allegations of strong ties between Hussein's Iraq and al-Qaeda or similar

networks. The search for WMDs ended in December 2004, and an inspection report submitted to Congress by U.S. weapons hunter Charles A. Duelfer essentially "contradicted nearly every prewar assertion about Iraq made by Bush administration officials."[32]

This chapter's Global Perspective discusses Israel's hunt for master bomb-maker Yehiya Ayyash, also known as "The Engineer." The manhunt is an instructive case on the response of security forces to an ongoing and imminent threat of terrorist violence.

GLOBAL PERSPECTIVE

ACTIONABLE INTELLIGENCE: ISRAEL AND THE HUNT FOR "THE ENGINEER"[a]

Yehiya Ayyash, a master bomb maker better known as "The Engineer," was a model activist within Hamas's cell-based organizational structure. Unlike PLO-style groups, Hamas required its operatives to organize themselves into small semiautonomous units. Ayyash was an al-Qassam cell (and later a "brigade") commander, but he had very few outside contacts and built his bombs in an almost solitary setting. He taught others to make bombs and how suicide bombers should position themselves for maximum effect.

The Engineer's first bomb was a Volkswagen car bomb that was used in April 1993. When Hamas began its suicide bombing campaign after the February 1994 Hebron massacre, Ayyash was the principal bomb maker. His bombs were sophisticated and custom made for each mission. They were particularly powerful compared to others previously designed by Hamas.

Ayyash was killed in January 1996. The cell phone he was using to carry on a conversation with his father had been booby-trapped by Israeli security agents and was remotely detonated. The assassination occurred as follows:

> Fifty grams of RDX [plastic] explosives molded into the battery compartment of a telephone had been designed to kill only the man cradling the phone to his ear. The force of the concentrated blast caused most of the right side of Ayyash's face to implode. . . . The booby-trapped cellular phone had been . . . so target specific, that the left side of Ayyash's face had remained whole. The right hand which held the telephone was neither burnt or damaged.[b]

The Engineer had been directly and indirectly responsible for killing approximately 150 people and injuring about 500 others.

Notes

a. Primarily from Samuel M. Katz, *The Hunt for the Engineer: How Israeli Agents Tracked the Hamas Master Bomber* (New York: Fromm International, 2001).

b. Ibid., 260–61.

CHAPTER SUMMARY

The Intelligence Community occupies a central role in maintaining a viable homeland security enterprise. Intelligence agencies are charged with distinct missions within the Intelligence Community and are led by the Central Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, and the Federal Bureau of Investigation. Intelligence coordination and cooperation are critically necessary to the success of homeland security, but on occasion, there have been problems and rivalries that have affected intelligence collection and analysis. Intelligence agencies perform a critical international role in securing the domestic

homeland security environment. The intersection of their missions with those of domestic agencies creates a large and intricate establishment for combating terrorism domestically and internationally.

DISCUSSION BOX

This chapter's Discussion Box is intended to stimulate critical debate about the possible use, by democracies and authoritarian regimes, of antiterrorist technologies to engage in surveillance.

Toward Big Brother?

Electronic surveillance by government agencies has become a controversial practice in the United States and elsewhere. The fear is that civil liberties can be jeopardized by unregulated interception of telephone conversations, e-mail, and fax transmissions by intelligence centers. Detractors argue that government use of these technologies can conceivably move well beyond legitimate application against threats from espionage and terrorism. Absent strict protocols to rein in these technologies, a worst-case scenario envisions intelligence intrusions into the everyday activities of innocent civilians. Should this happen, critics foresee a time when privacy, liberty, and personal security become values of the past.

Discussion Questions

1. How serious is the threat from abuses in the use of information collection technologies?
2. How should information collection technologies be regulated? Can they be regulated?
3. Is it sometimes necessary to sacrifice a few freedoms to protect national security and to ensure the long-term viability of civil liberty?
4. Should the same protocols be used for domestic electronic intelligence collection and foreign collection? Why?
5. What is the likelihood that new intelligence technologies will be used as tools of repression by authoritarian regimes in the near future?

KEY TERMS AND CONCEPTS

The following topics were discussed in this chapter and can be found in the glossary:

Central Intelligence Agency (CIA) 109
Defense Intelligence Agency (DIA) 117
DHS Office of Intelligence and Analysis (I&A) 118
Diplomatic Security Service 109
Director of National Intelligence 111
geospatial intelligence (GEOINT) 115
human intelligence (HUMINT) 114
imagery intelligence (IMINT) 115
Intelligence Community (IC) 108
measurements and signatures intelligence (MASINT) 115
National Counterterrorism Center (NCTC) 111
National Intelligence Priorities Framework (NIPF) 115
National Reconnaissance Office (NRO) 118
National Security Agency (NSA) 117
Office of the Director of National Intelligence (ODNI) 111
open source intelligence (OSINT) 115
Rewards for Justice Program 109
signals intelligence (SIGINT) 114

ON YOUR OWN

Get the tools you need to sharpen your study skills. SAGE edge offers a robust online environment featuring an impressive array of free tools and resources.

Access practice quizzes, eFlashcards, video, and multimedia at **edge.sagepub.com/martinhs3e**

RECOMMENDED WEBSITES

The following websites provide information about federal homeland security agencies:

Central Intelligence Agency: www.cia.gov

Office of the Director of National Intelligence: www.dni.gov

SITE Intelligence Group (USA): www.siteintelgroup.org

WEB EXERCISE

Using this chapter's recommended websites, conduct an online investigation of the role of intelligence agencies.

1. What are the primary documents explaining the underlying purpose and missions of intelligence agencies?
2. How would you describe the differences between intelligence agencies?
3. In your opinion, what practical options exist for coordinating national intelligence agencies?

To conduct an online search on research and monitoring organizations, activate the search engine on your Web browser and enter the following keywords:

"Intelligence agencies"

"Intelligence and the war on terrorism"

RECOMMENDED READINGS

The following publications provide discussions of intelligence agencies and their missions:

Andrew, Christopher. 1987. *Her Majesty's Secret Service: The Making of the British Intelligence Community*. New York: Penguin.

Bamford, James. 2001. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency, From the Cold War Through the Dawn of a New Century*. New York: Doubleday.

Berentsen, Gary. 2008. *Human Intelligence, Counterterrorism, and National Leadership: A Practical Guide*. Dulles, VA: Potomac Books.

Monje, Scott C. 2008. *The Central Intelligence Agency: A Documentary History*. Westport, CT: Greenwood.

Thomas, Gordon. 2009. *Gideon's Spies: The Secret History of the Mossad*. 5th ed. New York: St. Martin's Press.

Warrick, Joby. 2011. *The Triple Agent: The al-Qaeda Mole Who Infiltrated the CIA*. New York: Doubleday.