



فرماندهی کل قوا  
ستاد کل نیروهای مسلح  
دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

بسمه تعالی  
  
جمهوری اسلامی ایران

دقتربه زبان انگلیسی  
ویژه مصاحبه دوره دکتری (Ph.D)  
رشته حفاظت اطلاعات راهبردی  
سال تحصیلی ۱۴۰۱-۱۴۰۲

# Chapter 1

## **An Overview of Intelligence**

Intelligence is more than information. It is knowledge that has been specially prepared for a customer's unique circumstances. The word knowledge highlights the need for human involvement. Intelligence collection systems produce...data, not intelligence; only the human mind can provide that special touch that makes sense of data for different customers' requirements.

Captain William S. Brei  
*Getting Intelligence Right: The Power of Logical Procedure*

### **Chapter Objectives**

1. Demonstrate familiarity with the many definitions and uses of the term "intelligence."
2. Understand how intelligence enhances national security.
3. Summarize the relationship between the intelligence community and policymakers/decision-makers.
4. Recognize how the "reality" of intelligence work often differs from common perceptions and myths perpetuated in the popular media.
5. Understand the importance of "decision advantage" and how it can be achieved.
6. List and explain the five functions of intelligence agencies.

## Introduction

---

**Intelligence** has played a critical role in mankind since the earliest humans began to think and process information. Information and the intelligence drawn from that information directly influence the daily decisions of individuals, businesses, industry, the military, and the government. Nations have risen and fallen on the power of intelligence and the decisions that have resulted from it. Thus, the ability to know, anticipate, and plan is very powerful.

The hope of decision-makers is that intelligence will provide knowledge of quantitative factors and afford insight into the intangible. When that happens, intelligence can describe existing situations and identify or confirm capabilities that will shape future conditions.

Throughout the text, we will expand on the ideas presented in this chapter. One overriding theme that readers should keep in mind is this: however we examine intelligence, from the perspective of the public (government), military, or the private sector (business), its purpose is to provide that critical edge in decision-making that shifts the balance in favor of the decision-maker. This is a concept known as **decision advantage**, where one knows more than a competitor or adversary. This concept is very important in today's intelligence world. In a 2008 publication titled *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise*, the Director of National Intelligence (DNI) quoted Georgetown professor Jennifer Sims when describing the benefits of decision advantage:

...The key to intelligence-driven victories may not be the collection of objective 'truth' so much as the gaining of an information edge or competitive advantage over an adversary. Such an advantage can dissolve a decision-maker's quandary and allow him to act. This ability to lubricate choice is the real objective of intelligence. (Director of National Intelligence, 2008: 8)

## What Is Intelligence?

---

As we shall see, intelligence is itself a dynamic concept that does not have just one definition or application. As mentioned above, the ultimate purpose of the intelligence product is simple: provide an edge to the decision-maker. Intelligence is many things, but foundationally, its core mission is to provide knowledge of the world in which we live. This may come as a surprise to those weaned on spy movies and fiction—although the Intelligence Community (IC) does engage in covert and operational activities when the need arises, the production of knowledge is its main mission. At a conference your authors once attended, a senior IC official explained to students why the suave, fictional MI-6 operative James Bond may, in reality, be the world's worst spy. We include his explanation in Box 1.1.

### BOX 1.1 JAMES BOND: WORLD'S WORST SPY?

James Bond is a fictional spy created by Ian Fleming, who once worked for British Intelligence. Bond movies are wildly entertaining, with numerous action sequences and intense romances. However, at a conference attended by your authors, a prominent figure from an American intelligence agency once described why Bond may be the world's worst spy:

- Everyone knows who he is—the phrase “Bond, James Bond” brings instant recognition. In reality, spies need to keep their identities confidential.
- Bond causes a scene everywhere he goes—from car chases to shooting on the run, he wreaks havoc wherever he is. Real spies must remain discreet.
- He has questionable and frequent romantic relationships, often with agents from the other side. In reality, such actions can lead to compromising situations and blackmail.
- While intelligence agencies run on information, Bond never files reports. He seems to do all his talking with his fists.

## The Challenge of Defining Intelligence

No single definition of intelligence is accepted by all. The term itself is used in a variety of ways, which makes it difficult to come up with a single definition. Complicating the problem, different agencies have particular missions and operate under different rules. For example, the focus of the Central Intelligence Agency (CIA) is international. It has an entirely different set of guidelines than a domestic law enforcement organization, such as the Federal Bureau of Investigation (FBI). Hence, both define intelligence somewhat differently.

The title of a 2002 article by Michael Warner frames the issue nicely: “Wanted: A Definition of ‘Intelligence’” (Warner, 2002). Noting the many definitions that abound, Warner concluded that although definitions vary, the common purpose of the intelligence enterprise remains relatively consistent. Using the Hoover Commission of 1955 as an example, he noted that its simple definition seemed to do the trick: intelligence “deal[s] with all the things which should be known in advance of initiating a course of action” (Warner, 2002).

Although Warner may have been satisfied with that simple description, the issue remains unsettled. For example, the *International Dictionary of Intelligence* defines it as:

[T]he product resulting from the collecting and processing of information concerning actual and potential situations and conditions relating to domestic and foreign activities and to domestic and foreign or US and enemy-held areas. (Carl & Bancroft, 1990)

Contrast the above with the definition used by the FBI:

Simply defined, intelligence is information that has been analyzed and refined so that it is useful to policymakers in making decisions—specifically, decisions about potential threats to our national security. (Federal Bureau of Investigation, n.d.)

The 2007 publication *Joint Intelligence (JP 2-O)* provides yet another definition, one with a decidedly military spin:

The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. (Joint Chiefs of Staff, 2007: GL 11)

An examination of each definition makes one thing clear: agencies construct them to meet their particular needs and missions. For example, the FBI is concerned primarily with domestic and international threats confronting the homeland, what it defines as “potential threats to our national security.” The military, on the other hand, is concerned with “foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.”

In its 1999 *Consumers’ Guide to Intelligence*, the CIA provided this succinct definition:

Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us—the prelude to decision and action by US policymakers. (Central Intelligence Agency, 1999: vii)

Note that the CIA adds the requirement that intelligence should act as a “prelude to decision and action,” implying that it should not merely satisfy idle curiosity; according to this definition, intelligence must be useful for some larger purpose, generally one that serves the national interest. This sort of intelligence, which can empower a consumer toward some level of understanding or action, is often termed **actionable intelligence**. Some argue that *all* intelligence should strive toward this state.

Each of these definitions contains elements of the larger picture, and all have the benefit of brevity. Yet, none encompasses the wide range of activities carried out by today’s IC. A more comprehensive and illuminating definition appears in *Intelligence: From Secrets to Policy*, written by retired CIA analyst Mark Lowenthal:

Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers; the products of that process; the safeguarding of these processes

and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities. (Lowenthal, 2008: 8)

Lowenthal's definition is salient for several reasons. In the first place, it highlights the various aspects of the definition as commonly used today. Intelligence is a *process*, one that involves many steps. These will be discussed at length in Chapter 7 ("Putting It All Together: The Intelligence Cycle"). As a process, it is also dynamic—that is, intelligence activities do not stop.

Intelligence is also a *product*, such as national intelligence estimates that detail analyses of particular strategic issues or the Presidential Daily Brief, which is a succinct rendering of important issues prepared specially for the President of the United States. Many, but not all, of these products are classified—that is, only those individuals with a sufficient security clearance and a need-to-know may access them.

Intelligence is also about protecting what we know—what is termed *counterintelligence*. Achieving decision advantage is not just about learning as much as possible about an adversary; it is also about protecting one's own information. Just as a football team needs to play both offense and defense well, the IC needs to both protect and acquire—if either is not achieved, decision advantage can be lost.

Finally, intelligence often refers to the *community* that collects and analyzes important information and disseminates it as intelligence. Chapter 3 ("The IC Today") discusses the myriad parts of today's IC: the 17 agencies that make up the nucleus of the federal intelligence world; the other federal, state, and local agencies that also participate in the effort; and the private sector, with its huge resources and wide breadth.

## Information and Intelligence

---

At this point, readers should realize that we have made a great effort to separate the terms "information" and "intelligence." In fact, they are not synonymous. **Information** is unprocessed material of every description that can be used to produce intelligence. It is, in essence, "raw data." Since intelligence is derived from information, it shares many attributes of information. Information, and the intelligence that results from it, is perishable. Information will often be incomplete, sometimes confusing, and contradictory. Not all information will be important or even relevant, and much of it may be inaccurate or misleading. Too much information can be as harmful as too little. With all information, we seek not a large amount, but rather to have the right information available when needed.

The world of intelligence is one fraught with ambiguity and uncertainty—agencies rarely have enough good, reliable information upon which to make ironclad judgments. In addition, adversaries also want to gain decision



advantage. As a result, they feed **disinformation**, or intentionally false information, in the hope of disguising their true activities or intentions.

Can raw information ever rise to the level of intelligence? The dividing line is far from clear. However, if a member of the IC received uncorroborated and unverified information that someone had planted a nuclear device across town that would detonate in 30 minutes, unless they had very good reason to doubt its authenticity, they would act as if it were intelligence—that is, they would assume that both the source and information might be credible and would take action as appropriate. The risk of acting otherwise would be too great. Ideally, all information will undergo the process described in Chapter 7 (“Putting It All Together: The Intelligence Cycle”). However, operational realities and short deadlines often preclude that. Instead, the trend indicates that more and more decision-makers want to see raw data rather than wait for a finished product. Although their impatience is understandable, some critics worry that this shortcuts the important “value added” that analysts with a deep understanding of the subject provide.

## Types of Intelligence

---

Intelligence products can be divided into various categories depending on their focus or scope. Some products are **tactical**, which means they are designed for near-term use, usually by on-the-ground personnel. For example, an army unit on patrol would be interested in whether the enemy is over the next hill; likewise, drug agents may want to know the background of the suspected drug dealers they are about to meet. Such intelligence has a great deal of immediacy. As a result, the process by which it is converted from information to intelligence is often short-cut. In some cases, this is necessary and desirable. For example, if a Predator unmanned aerial vehicle (UAV) spotted what appeared to be an enemy patrol in Afghanistan about to ambush coalition forces, it would be imprudent not to warn the soldiers in the field. However, haste can lead to miscalculations; on more than a few occasions, “friendly fire” has killed allies or civilians mistaken for enemy combatants on the battlefield.

Another type of intelligence, generally consumed by senior leaders and policymakers, is **strategic**. This refers to longer term issues that have large implications and potential consequences (see Figure 1.1). It may entail broad topics, such as economic projections, and often looks out into the future. For example, the DNI has produced a series of studies concerning whether Iran intends to produce nuclear weapons. This is, of course, an issue that concerns individuals at the highest levels of the chain-of-command, including the President, who have to make the serious decision of whether to carry out a military strike. Usually, strategic products require much more lead time than tactical ones. By definition, they require meticulous research and



**FIGURE 1.1** Fort McClellan, AL. Lt. Col. Keith Calhoun (standing left), Deputy Chief of Operations, 167th Theater Sustainment Command (TSC), briefs Lt. Gen. Guy Swan III (seated, center of table), Commanding General, U.S. Army North, on 167th TSC's capabilities and unit structure, January 20, at 167th TSC headquarters, Fort McClellan, AL. Often for decision-makers, strategic and tactical intelligence go hand-in-hand. (Courtesy of U.S. Army photo by Sgt. Joshua Ford, U.S. Army North PAO.)

analysis, given their seriousness. The highest level strategic product disseminated by the U.S. IC is a National Intelligence Estimate, further described in Chapter 11. (“Writing and Briefing for the Intelligence Community”). Multiple analysts working for various agencies prepare these products. They go through an exceptional preparation and review process to ensure that the information is as correct as possible and that the analysis is solid.

A third type of intelligence, termed **operational** intelligence, is often used by the military. This type falls somewhere between tactical and strategic and is usually used at a battalion or expeditionary force level.

Intelligence can also be categorized based on the area it covers. The IC draws a sharp distinction between **foreign** and **domestic** intelligence. The reason for this should be obvious—those residing in the United States—“U.S. persons”—are afforded significant rights under the Constitution; these same rights do not apply to non-U.S. citizens residing overseas.

According to Title 50, United States Code 401a, which has its origin with the National Security Act of 1947, foreign intelligence is defined as:

[I]nformation relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (Government Printing Office, 2009)



Foreign intelligence exists to provide information to decision-makers at all levels of government so that they can apply the power they have at their disposal more precisely. Agencies such as the CIA, the Defense Intelligence Agency (DIA), and the National Security Agency (NSA) have a foreign mission—they are not permitted to focus on domestic intelligence issues.

Domestic intelligence agencies exist to provide the same service to policy-makers who wield power domestically. Even though a single agency could collect and analyze intelligence information both overseas and at home, as the Soviet Union's KGB did, in the U.S., foreign and domestic intelligence collection is separated to protect domestic civil liberties. Agencies such as the FBI and the Drug Enforcement Administration (DEA) have domestic powers; each also stations personnel overseas to work with foreign law enforcement and intelligence organizations (Marrin, 2003).

## Functions of Intelligence Agencies

---

Intelligence agencies engage in up to five discrete activities. Some agencies, such as the CIA, engage in all five; others perform fewer. In his book *Intelligence: From Secrets to Policy*, Lowenthal (2009) discusses four: collection, analysis, covert activities, and counterintelligence. To this list, we add a fifth: the management of intelligence.

**Collection** is the act of gathering information and data. In the IC, the collection platform is often used to describe the type of intelligence that is produced. This has given rise to the naming convention of the “INTs,” which is the suffix attached to an acronym describing the type of information collected (acronyms are ubiquitous in the intelligence world). For example, HUMINT refers to “human intelligence,” or information obtained from human sources. Even though the suffix “INT” is used, readers should be cautioned that what is being gathered is information, not intelligence. As discussed above, information must generally go through a process to become intelligence.

The explosion in technology over the past 20 years has given rise to new sources of information—satellites, computers, cell phones, and the like provide scores of data. Today, the issue for the IC is not lack of information; rather, it is “separating the wheat from the chaff”—finding one piece of information among the terabytes that, when linked with other data, will provide the answers that policymakers seek. Collection issues are examined in Chapter 4.

Raw information in and of itself usually does not equal intelligence. First, it must be linked, interpreted, and contextualized; this is the process of **analysis**. Perhaps surprisingly, many experts blame recent intelligence lapses, such as the failure to prevent the 9-11 attacks and the false conclusion that Saddam Hussein possessed weapons of mass destruction, on problems with

analysis, not collection. The phrase “connecting the dots” has come to epitomize the rather simplistic conclusion that, if only analysts had paid more attention and had better shared information, they could have prevented the attacks of 9-11. Although this conceivably may have been the case, it severely underestimates the difficulty in performing analysis. As previously explained, information is often ambiguous and of questionable reliability; the sheer volume that is received makes it difficult to prioritize what is the most important. Chapter 5 describes barriers to analysis, whereas Chapter 6 discusses strategies the IC has used to improve its analytical methods.

The next function that IC agencies engage in is **counterintelligence** (CI), or the protection of information and intelligence. There are many ways this can be accomplished. The first is primarily defensive—information is assigned a level of classification based on its sensitivity and potential harm to national security if released. Most readers will be familiar with the terms “confidential,” “secret,” and “top secret.” These are levels of security ranging from low to high. To access classified information, individuals must possess security clearances equal to or greater than the intelligence they wish to view. To receive a clearance, a person must successfully pass an in-depth background investigation. This is a detailed process where agencies examine every facet of an individual’s life. Additionally, drug tests and polygraph examinations are often included as part of the investigation.

Counterintelligence also has an offensive aspect. Every agency of the IC has a security office responsible for seeking out security breaches and leaks. Unfortunately, the United States has had its share of double agents who betrayed the trust of the country by providing classified information to adversaries. Of course, this is what HUMINT is all about—CIA Case Officers attempt to convince citizens of foreign countries to do exactly the same thing for the benefit of the United States. Individuals caught spying are usually subject to harsh punishments—in many countries, the penalty is death. In the United States, spies such as Robert Hanssen and Aldrich Ames often receive a sentence of life in prison. The FBI is the lead agency in the United States for conducting counterintelligence; it is the Bureau’s second priority, just behind the prevention of terrorism.

Another offensive way to carry out CI is by disseminating disinformation. If successful, this can tie up an adversary’s resources and send them in false directions. It can also mislead them about intentions or capabilities. CI is discussed in Chapter 8.

When many people think of the IC, they envision **covert operations**, such as the failed Bay of Pigs operation or the killing of Osama Bin Laden. In fact, the IC carries out covert ops relatively infrequently and only with permission from the highest authorities. The key characteristic of a successful covert op is **plausible deniability**, where the operation itself cannot be traced back to the U.S. government. Oftentimes, this deniability fails, especially when

the operation proves unsuccessful. There has been much debate concerning whether covert operations have, in the long run, helped or hurt U.S. interests. Proponents claim that much good has been accomplished over the years, often out of the glare of media scrutiny. Others maintain that these types of activities are often discovered and, even when successful, lead to undesirable and unintended consequences. For example, in 1953, the CIA engineered a coup that led to the overthrow of the popularly elected prime minister of Iran. Years later, however, another coup deposed the U.S.-selected leader and led to the formation of an anti-American theocracy that persists to this day. Presently, Iran is a major foreign policy challenge for the United States. Covert operations are discussed in Chapter 9.

Finally, IC agencies engage in **intelligence management**. This consists of several phases. The first involves organizing and processing the voluminous amounts of data that arrive daily. It also involves storing intelligence once produced. There are literally libraries worth of information and intelligence that the IC stores and maintains because one never knows what may prove important someday. Lastly, managing intelligence includes its proper dissemination. This is a critical and sometimes overlooked step in the process. Intelligence that is not delivered properly will be ignored. Ignored intelligence is no better than intelligence that was never produced. In Greek mythology, Cassandra was a beautiful noblewoman who was granted the gift of prophecy by Apollo. However, because she spurned his romantic advances, he placed a curse on her that no one would believe her predictions. Analysts who cannot articulate their thoughts properly will suffer the fate of Cassandra.

As a result, the IC places a great deal of emphasis on writing and briefing. Writing must be concise, clear, and accurate. Important information, such as one's conclusion, is rendered first. This style is termed **bottom line up front (BLUF)**. Because policymakers are busy people, they generally do not have time for long-winded explanations. This holds true for both writing and briefing—an experienced briefer will get to the main points quickly while avoiding “fluff.” We discuss management in Chapters 7 (“Putting It All Together: The Intelligence Cycle”) and 11 (“Writing and Briefing for the Intelligence Community”).

## **Policymakers and Decision-Makers**

In this text, we use the terms “policymaker” and “decision-maker” interchangeably. We note, however, that they do not necessarily mean the same thing. A decision-maker is, as the name implies, one who has to make decisions, oftentimes for an agency or organization. This can occur at both the strategic and tactical levels. A policymaker, on the other hand, makes decisions that affect policy—in almost every case, this means a decision at the

strategic level. Every policymaker is a decision-maker, but the opposite is not necessarily true. Each, however, is a potential consumer of intelligence.

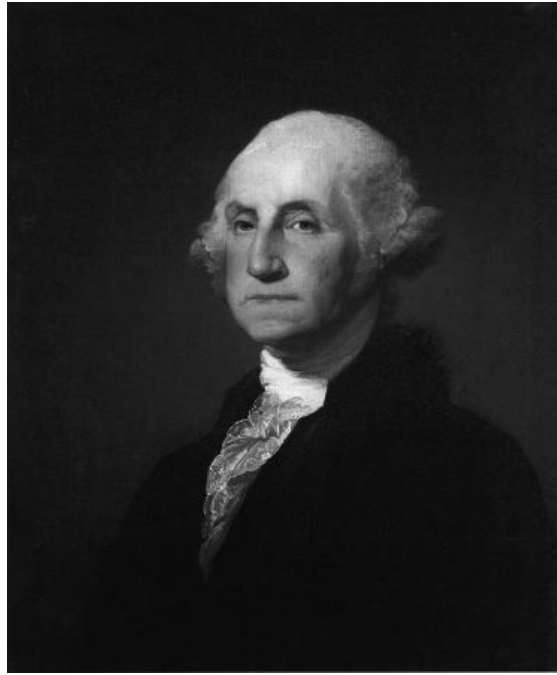
It is important to understand the relationship between the IC and policymakers/decision-makers. In fact, those who produce intelligence should refrain from formulating policy—that is not their job. Instead, intelligence professionals should describe the world around them in the most objective way possible, free from political or personal concerns. It is their responsibility to “tell it like it is” to the decision-maker. Occasionally, this involves passing along bad news; for example, telling a policymaker that his or her plans or policies are not achieving their desired ends. This takes a great deal of bravery—no one likes hearing bad news. Given the political intrigue that is often found in organizations, the IC analyst may be the *only* individual who tells the boss unfortunate news. This is the beauty and the power of the position—good decisions can only be made in honest circumstances. To that end, the brave analyst, one who is willing to speak the truth, may be the best friend policymakers have, whether they recognize it or not.

This relationship can prove quite tricky. In a very real sense, the IC professional and policymaker share a producer–consumer relationship. Policymakers are under no obligation to “buy” what the IC has to “sell.” The IC’s product is, of course, its intelligence. If the intel provides a value-added component, a wise policymaker will continue to access and utilize it. However, if it appears to be of limited utility, the policymaker will soon begin to ignore both it and the messenger; the analyst will lose ever-important **access** to the consumer. In this case, they will truly become a Cassandra—even their most well-constructed analysis will be for naught.

This is complicated by the fact that many policymakers feel that they already have a good “handle” on the subject being analyzed. Some whose level of knowledge may be no deeper than that obtained by watching television news may feel that they have all the answers and that analysts, even those with decades of experience, may have little to offer.

As one can imagine, this can become a difficult situation. There is no perfect solution. Even looking at presidents over time, one sees widely differing relationships with the IC. Some loved covert operations, whereas others refused to engage in them. Some insisted on regular briefings and meetings, whereas others would go for long periods of time without significant contact. To a large extent, this appears to have been driven by personality and experience. For example, the first President Bush was a former director of the CIA before his ascension to the Presidency. He had a familiarity with intel matters and an appreciation for what the IC could do. As a result, his contact with intelligence agencies was frequent. President Clinton, on the other hand, lacked this level of familiarity and comfort; his dealings were much more sporadic.





**FIGURE 1.2** A portrait of George Washington, one of the first U.S. leaders to recognize the value of intelligence. By artist Gilbert Stuart, circa: 1796. Currently housed at the Sterling and Francine Clark Art Institute, Williamstown, MA, USA. Public Domain. (Courtesy of Wikipedia Commons.)

## **Intelligence Foundations in U.S. Government**

---

Intelligence has been a function of the government since the beginning of the republic. George Washington (Figure 1.2) put intelligence to decisive military use during the American Revolution; it has been an integral part of U.S. military operations ever since. Over the next 200 years, the intelligence of the U.S. government evolved into an elaborate and complex collection of agencies with global capabilities. The rich history of the evolution of U.S. intelligence will be discussed in Chapter 2.

## **U.S. Intelligence Community**

---

The U.S. IC is a coalition of 17 agencies and organizations within the executive branch that works both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities. The primary mission of the IC is to collect and convey the essential information that the president and members of the policymaking, law enforcement, and military communities require to execute their appointed duties. The 17 agencies possess a wide range of capabilities and intelligence needs themselves. In addition to these 17 organizations, the IC also consists of other federal, local, state, and private organizations, all of which are described in Chapter 3.



## Purpose of Intelligence

---

The decision-maker generally wants intelligence to answer three basic questions: (1) What capabilities do our adversaries possess? (2) What are their intentions—in particular, what is the most dangerous thing they may do? (3) What effect might all this have on our ability to accomplish our national goals?

Obviously, answers to these questions are very important, especially when they concern such volatile situations as Iran or North Korea. Perhaps the biggest value added for policy-makers is that good intelligence reduces uncertainty—although it may not answer every question, it allows leaders to make better decisions; indeed, it provides them with decision advantage.

## Limitations of Intelligence

---

There are limits to what intelligence can provide. Intelligence may reveal “secrets” (information that is knowable but hidden); however, some situations remain “mysteries,” and agencies cannot discern their true nature. What a foreign leader is thinking, for example, cannot be known unless the leader makes it known. Whether the same foreign leader will even be in power in a year’s time is a “mystery” that only time will reveal.

## Conclusion

---

There is nothing mysterious about intelligence. Although collection and production may involve the use of high technology sensors and networks, good intelligence is primarily the result of solid headwork and legwork. Good intelligence begins with decision-makers clearly identifying their concerns and needs. It is developed through the focused collection of information, thorough study, and, most importantly, through effective analysis and synthesis. The result is an intelligence product that provides knowledge, reduces uncertainty, and supports effective decision-making.

For the United States today, intelligence is more important than ever given the current threat environment. Challenges are global and often emanate from transnational enterprises that rely on sophisticated information technology. They transcend geographic boundaries as well as the boundaries of authorities in the U.S. national security infrastructure. In this environment, having the right intelligence at the right time is essential to protecting national security.

### *Questions for Discussion*

1. How would you define “intelligence?” What factors did you consider in formulating this definition?
2. Is there really a big difference between “intelligence” and “information?” Why or why not?

3. Of the five functions of intelligence agencies discussed in the chapter, which is the most important? Why?
4. The relationship between the policymaker and intelligence professional is often described as a “consumer–producer” relationship. Is this a good analogy? Why or why not? Can you think of a better description?
5. We briefly discussed the limitations of intelligence in the chapter. Can you think of some others?
6. The IC receives billions of dollars of funding every year; between the public and private sectors, it is a massive undertaking. Yet, it has had several big failures, such as not preventing the 9-11 attacks and not foreseeing the fall of the Soviet Union in the latter part of the twentieth century. Why do you think this was the case?

## Key Terms

---

**Access to the decision-maker**

**Actionable intelligence**

**Analysis**

**Bottom line up front (BLUF)**

**Collection**

**Counterintelligence**

**Covert operations**

**Decision advantage**

**Domestic intelligence**

**Foreign intelligence**

**Information**

**Intelligence**

**Intelligence management**

**Operational intelligence**

**Plausible deniability**

**Strategic intelligence**

**Tactical intelligence**

## References

---

- Brei, W. (1996). *Getting intelligence right: The power of logical procedure*. Washington, DC: Joint Military Intelligence College.
- Carl, L., & Bancroft, E. (1990). *The international dictionary of intelligence*. Mclean, VA: Maven Books.
- Central Intelligence Agency. (1999). *A consumer's guide to intelligence*. Langley, VA: Central Intelligence Agency.
- Director of National Intelligence. (2008). *Vision 2015*. Retrieved October 15, 2015, from [http://www.dni.gov/Vision\\_2015.pdf](http://www.dni.gov/Vision_2015.pdf) on 12/31/2009.
- Federal Bureau of Investigation. (n.d.). Intelligence defined. Federal Bureau of Investigation. Retrieved December 28, 2011, from <http://www.fbi.gov/about-us/intelligence/defined>.
- Government Printing Office. (2009). *United States Code Title 50— War and national defense*. Retrieved January 3, 2012, from <http://www.gpo.gov/fdsys/pkg/USCODE-2009-title50/html/USCODE-2009-title50.htm>.

- Joint Chiefs of Staff. (2007). *Joint Publication 2-O: Joint Intelligence*. Retrieved December 29, 2011, from [http://www.fas.org/irp/doddir/dod/jp2\\_0.pdf](http://www.fas.org/irp/doddir/dod/jp2_0.pdf).
- Lowenthal, M. (2008). *Intelligence: From secrets to policy* (4th ed.). Washington, DC: Congressional Quarterly Press.
- Marrin, S. (2003). Homeland security intelligence: Just the beginning. Retrieved May 6, 2010, from <http://www.homelandsecurity.org/journal/Articles/Marrin.html>.
- Warner, M. 2002. Wanted: A definition of “intelligence.” *Studies in Intelligence*, 46. Retrieved May 6, 2010, from <http://www.homelandsecurity.org/journal/Articles/Marrin.html>.

# Chapter 2

## History of Intelligence in the United States

Whether the object be to crush an army, to storm a city, or to assassinate an individual, it is always necessary to begin by finding out the names of the attendants, the aides-de-camp, the door-keepers and sentries of the general in command. Our spies must be commissioned to ascertain these.

Sun Tzu  
*The Art of War*

### Chapter Objectives

1. Explain why the United States did not develop a robust, sustained intelligence capability until the twentieth century.
2. Trace the history of early American intelligence efforts from the Revolutionary War up until World War II.
3. Explain how the “strategic surprise” of Pearl Harbor convinced the United States that it needed to enhance its intelligence capabilities.
4. Describe how the Cold War was a “war of intelligence” and how it shaped the development of American intelligence agencies.
5. Explain how intelligence “failures,” such as the excesses of COINTELPRO and Operation CHAOS, and the spy scandals of the 1980s affected intelligence efforts.

6. Identify some reasons why the United States was not able to anticipate and thwart the attacks of September 11, 2001.
7. Describe how historical events have shaped the American intelligence efforts of today.

## Introduction

---

In contrast to Europe, the United States has not always had a strong, sustained intelligence effort. Thanks primarily to its nonthreatening neighbors to the north and south and oceans to the east and west, the United States has not faced existential threats. Additionally, the Bill of Rights and privacy have long been staples of the American republic. Spying is, by definition, a surreptitious and invasive activity; until recently, the federal government limited its use. This is not to say, however, that America has never engaged in intelligence collection. Indeed, over the years, the United States has enjoyed great success in the intelligence arena; it has also suffered some catastrophic failures, such as the attacks of September 11, 2001 and the surprise bombing of Pearl Harbor in 1941. To understand why the intelligence community (IC) today is structured the way it is, one must first understand its history.

## Revolutionary War to Civil War

---

George Washington was no stranger to intelligence. During the Revolutionary War, he set up both the **Secret Committee** and the **Committee of Secret Correspondence**, which reported on British troop movements, carried out various covert activities, and conducted sensitive negotiations with foreign governments. Washington knew that the British army was highly organized and well supplied; he realized that he needed the decision advantage described in Chapter 1 (“An Overview of Intelligence”) if America was to prevail. Part of this advantage consisted of keeping valuable information out of the hands of the enemy. Therefore, in 1776, Congress passed the First Espionage Act, which made “lurking as spies in or about the fortification or encampments of the armies of the United States” punishable by death (Central Intelligence Agency, 2007a).

There were both intelligence heroes and villains in America’s struggle against the British. One of the heroes was young Nathan Hale, who agreed to go behind enemy lines in the Battle of Long Island to gather information. Almost immediately, he was captured and hanged; legend has it that, on the gallows, he uttered the famous words: “I regret that I have but one life to lose for my country.” Today, a statue of Hale can be found on the campus of the Central Intelligence Agency (CIA)’s headquarters in Langley, Virginia.

Once the Revolutionary War ended, Washington did not form a permanent American intelligence service. Instead, in the early days of the republic,

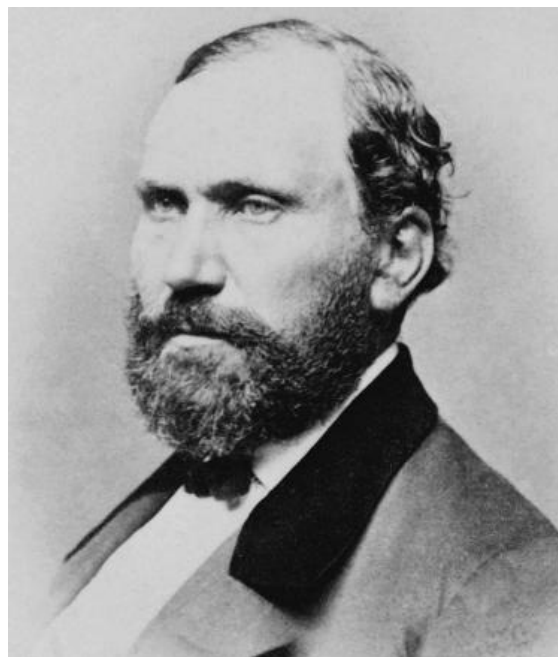


Presidents ordered spying and covert activities as the need arose, such as it did during the War of 1812 and the Mexican War of 1846. However, in neither case were American intelligence efforts nearly as successful as they had been during the Revolutionary War.

## Civil War to World War I

Both the North and the South set up intelligence operations during the Civil War. For the most part, military commanders were given wide discretion in how they gathered intelligence and used spies. For example, the Confederacy employed Belle Boyd and Rose O'Neal Greenhow, who gleaned valuable information from Union officers and passed it on to southern forces. In some cases, their intelligence was crucial in helping the Confederates win decisive victories.

Not all spies were employed by the government. In 1850, Allen Pinkerton (Figure 2.1) set up his famous detective agency for the purpose of allowing businessmen to covertly keep track of their employees. In 1861, the Pinkertons allegedly foiled a plot to assassinate President-elect Abraham Lincoln in Baltimore, Maryland. Although historians debate whether the plot was in fact real, the buzz it generated provided great publicity for the agency, which went on to guard Lincoln throughout the Civil War. Pinkerton detectives also worked as spies and agents for Union Major General George B. McClellan and ran his military intelligence service (Central Intelligence Agency, 2007b).



**FIGURE 2.1** Allan Pinkerton, circa 1861. Library of Congress Prints and Photographs Division, Washington, D.C. 20540. (Courtesy of Wikipedia Commons.)

Perhaps the most interesting intelligence operations of the War involved Harriet Tubman, famous for her work with the Underground Railroad. Tubman also served as an armed scout and a spy and helped lead a covert operation in South Carolina that freed 700 slaves. In addition, she made sure that runaway slaves escaping to the North via the Underground Railroad provided information on activities they had observed. In some cases, she and others were able to convince freed slaves to return to the South to engage in espionage and surveillance. The information provided by Tubman and her peers became known as the **Black Dispatches** and provided much valuable intelligence to the North.

The Civil War also witnessed new types of intelligence collection, brought about by increasingly improving technologies. For example, Thaddeus Lowe flew above the battlefields in a balloon and reported on Confederate troop movements. Not everyone appreciated his efforts. Amazingly, President Abraham Lincoln had to convince his doubting generals that this form of collection was a good idea (National Air and Space Museum, 2000).

By the latter part of the nineteenth century, the Navy recognized that it technologically lagged behind the navies of the European powers. In 1882, it formed the Office of Naval Intelligence, whose primary mission was to help modernize U.S. forces by learning the secrets of other countries; it also gathered military intelligence during the Spanish–American War (Office of Naval Intelligence, n.d.). The Army soon followed suit and formed the Military Information Division in 1885.

## Law Enforcement Intelligence: The Palmer Raids

---

As World War I neared, there was great upheaval throughout much of the world. With the Russian Revolution only a few years off, workers from around the world organized to oppose what they considered to be oppressive conditions foisted upon them by wealthy business owners and capitalists. One such group, which shared many views in common with the Communists, was known as the **anarchists**. In the United States, many anarchists were immigrants who lacked citizenship. In 1914, radical anarchists began a series of bombings that targeted government authorities and businesses. Several deaths resulted from these attacks, which included a horrific 1920 bombing in the Financial District of New York City that claimed the lives of 38 and injured more than 400 (Bailey & Kennedy, 1994).

By 1919, Attorney General Alexander Mitchell Palmer decided that something had to be done at the federal level to address anarchist violence. He turned to a small, largely unknown agency in the Department of Justice (DOJ) known as the Bureau of Investigation (BOI). The BOI had been founded in 1908 by Attorney General Charles Bonaparte; its primary

mission was to investigate white collar crime and enforce the Mann Act, which concerned interstate prostitution. Palmer turned to a young lawyer in the DOJ named J. Edgar Hoover, whom he believed was best suited to deal with the anarchists. It proved to be a choice that would have ramifications for years to come.

From 1919 until 1921, the BOI, the Immigration and Naturalization Service, and local police departments carried out a series of raids against suspected anarchists; many of them were jailed and a large number were deported, often with little or no due process. Dubbed the **Palmer Raids**, they were soon judged by many citizens to have been excessive; groups such as the American Civil Liberties Union strongly objected to the treatment doled out, in many cases to individuals who were likely innocent (Murray, 1955; Irons, 1999).

The BOI became the Federal Bureau of Investigation in 1935, with Hoover serving as its director until 1972; as history would prove, he never lost his zeal for investigating suspected radicals and subversives.

## World War I to Pearl Harbor

Immediately after World War I, the United States realized that it needed to enhance its intelligence capabilities. By this time, America had developed the ability to intercept diplomatic communications, but a problem remained: most messages were coded. To solve the dilemma, the State Department and military collaborated on a project officially named the Cipher Bureau, but generally referred to as the **Black Chamber**. Headed by cryptanalyst Herbert O. Yardley, the Black Chamber decrypted the message traffic of foreign governments, to include those of the Japanese diplomatic service; this provided the United States with a negotiating edge during the 1922 Washington Conference (Hannah, 1981). Despite its success, the Black Chamber lasted only until 1929. In shutting it down, Secretary of State Henry L. Stimson famously remarked that “gentlemen don’t read each others’ mail,” once again underscoring America’s seeming repugnance toward intelligence (Knowledgerush, n.d.).

Franklin Roosevelt was elected President of the United States in the middle of a great economic depression. Roosevelt had mixed feelings regarding intelligence. On the one hand, he directed FBI Director J. Edgar Hoover (Figure 2.2) to aggressively investigate the German American Bund, Asians, Communists, and subversives in the United States. However, he was less than aggressive when it came to other types of collection. With improving technology, signals intelligence (SIGINT) was becoming a viable way to monitor a potential enemy’s communications. Roosevelt, however, seemed reluctant to pursue it in any sustained manner. This would prove disastrous; had America been able to break the Japanese naval code, it is entirely



**FIGURE 2.2** First director of the FBI, J. Edgar Hoover. (Courtesy of Wikipedia Commons.)

possible that forewarning of the impending Japanese attack on Pearl Harbor could have been provided. As it turned out, the bombing on December 7, 1941, took America by surprise.

## World War II

Despite the fact that the Pearl Harbor attack came as a shock, the United States had been preparing for war for some time. Even before the attacks, Roosevelt realized that he needed better intelligence but faced several obstacles. Chief among these was the fragmented nature of the American intelligence enterprise. Disparate agencies, such as the FBI and the military, rarely worked together and generally did not share information. In mid-1941, Roosevelt created the position of **Coordinator of Information (COI)**, whose mission was to better integrate intelligence among agencies and to encourage information sharing, not an easy task given the often competitive relationship that existed. As the first COI, Roosevelt chose William “Wild Bill” Donovan, a Medal of Honor recipient, successful lawyer, prosecutor, and diplomat.

By 1942, it had become clear that the Office of the COI needed to expand to support the war effort. Reappointing Donovan to the Army, Roosevelt



placed him in charge of a new organization, the **Office of Strategic Services (OSS)**. The OSS was a true intelligence service. At its height, it boasted 24,000 employees and a budget exceeding \$10 million. During the war, OSS operatives engaged in all sorts of operations. They trained and equipped underground movements, inserted spies into enemy territory to gather information, and engaged in sabotage.

On the home front, the FBI investigated suspected foreign spies and saboteurs. One of its most famous cases was the capture of members of the Nazi **Operation Pastorius** ring, who had landed on the beaches of Long Island, hoping to destroy American factories and economic targets.

The Bureau also operated the **Special Intelligence Service (SIS)** during the war. Because the CIA did not yet exist, the United States needed an intelligence arm to monitor the large German population in Central and South America, many of whom were sympathetic to the German cause. In due course, hundreds of Special Agents were assigned south of the border to keep track of potential spies and saboteurs. According to the FBI:

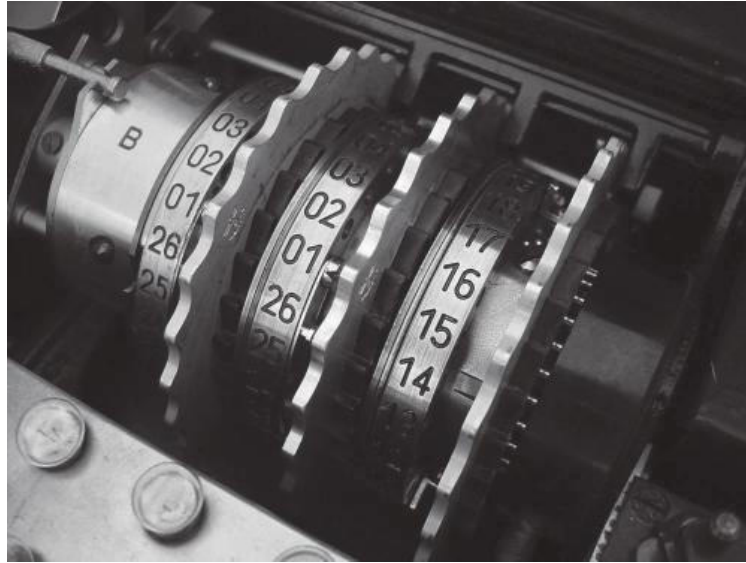
By 1946, [the SIS] had identified 887 Axis spies, 281 propaganda agents, 222 agents smuggling strategic war materials, 30 saboteurs, and 97 other agents. It had located 24 secret Axis radio stations and confiscated 40 radio transmitters and 18 receiving sets. And the FBI had even used some of these radio networks to pass false and misleading information back to Nazi Germany. (Federal Bureau of Investigation, n.d.(a))

Intelligence proved critical to the war effort. One of the allies' greatest successes was the breaking of the sophisticated Nazi cipher that was generated on its "enigma" machines (see Figure 2.3a and b). Dubbed **Project Ultra**, cryptanalysts at Bletchley Park in England worked feverishly to decode as many German messages as possible. Shrouded in great secrecy so as not to alert the Germans that their code had been broken, the Project Ultra messages proved crucial in assisting the allies with operations throughout the war. Allied code-breakers also managed to break the Japanese "Purple" code, which assisted in gaining victories in naval engagements in the Pacific.

Despite its great success, President Truman disbanded the OSS after the war. However, unlike the past, experts knew that the United States needed a permanent intelligence agency beyond that provided by the military. Even though the world was technically at peace, it had become a dangerous and complicated place. With both sides soon to be armed with weapons that could wreak unfathomable harm, a new type of war was about to emerge. Unlike the "hot" one that had just concluded, this one would be fought with spies and on "proxy" battlefields. The role of intelligence was about to achieve a level of importance unprecedented in American history.



(a)



(b)



**FIGURE 2.3** (a) Enigma rotor assembly. (b) A World War II enigma cipher coding machine. (Both images courtesy of Shutterstock.com.)

## The Cold War

The world's first Communist state, the Soviet Union, was formed through revolution in 1917. In just about every way, the values of Communism and those of capitalism stood in sharp contrast. Of great concern to the West was the notion that the Communist revolution was an ongoing enterprise—it would not cease until all nations of the world had been “liberated” and brought within the Communist sphere of influence.

Even before the end of World War II, Western nations realized that they would soon be in competition with their ally. This point was driven home forcefully in a series of conferences in which Allied leaders planned the post war world. At the end of the day, countries in Eastern Europe were ceded to the Soviets, whereas those in the West fell under the influence of democracies. Germany was divided in half, with West Germany going to the West and East Germany falling under the Communists. The capital city of Berlin, which was geographically located inside East Germany, was likewise divided in half, with West Berlin allowed to exist as a democracy and East Berlin aligned with the Soviets.

The United States did not wait until the end of the war to begin gathering intelligence on the Soviets. In 1943, the U.S. Army, working with British intelligence, initiated an aggressive SIGINT operation called **Project Venona**, which monitored Soviet communications until 1980. Among other things, Venona provided information that a New York City-based espionage ring had provided atomic secrets to the Soviets, allowing them to detonate an atom bomb in 1949.

One of the first memorable events of the **Cold War** came in a 1946 speech delivered by Winston Churchill in which he declared that an **Iron Curtain** had descended over Europe, dividing the “free” countries from those controlled by the Communists. The phrase “iron curtain” would resonate for the next 40 years, signifying that the world had become bipolar, with two opposing philosophies seeking to expand their spheres of influence over nonaligned “third world” countries.

In 1946, the Deputy Chief of the U.S. Mission in Moscow, George Kennan, articulated what came to be America’s strategy for dealing with the Soviets; rather than trying to work with them or confront them in battle, a more realistic goal was to “contain” their expansion. The philosophy of **containment** would guide U.S. foreign policy throughout the Cold War, directing intelligence and diplomatic efforts and prodding America into two major military actions and several conflicts.

By 1949, the Soviets had developed their own atomic bomb, helped along by espionage directed against the United States. A New York City-based spy ring, run by the husband-and-wife team of Julius and Ethel Rosenberg (Figure 2.4), was arrested for passing nuclear secrets to the Soviets; the Rosenbergs were found guilty and executed for those crimes in 1953. The case remained controversial for many years, with scores of citizens convinced that the Rosenbergs were innocent. What could not be revealed at the time, however, was that Venona intercepts had confirmed their guilt.

With both sides possessing nuclear weapons, direct military confrontation became unthinkable. The role of intelligence for both nations and their alliances gained even greater importance. As the United States and the Soviet Union raced to develop and stockpile nuclear, chemical, and



**FIGURE 2.4** Julius and Ethel Rosenberg, separated by heavy wire screen as they leave U.S. Court House after being found guilty by jury, 1951. (Courtesy of Roger Higgins, photographer from *New York World-Telegram and the Sun*. Library of Congress Prints and Photographs Division and Wikipedia Commons.)

biological weapons, the world balanced on the edge of another global conflict. The United States adopted the military strategy of **Mutually Assured Destruction**, in which each side was deterred from going to war, lest both be destroyed in the process.

Over the next 40 years, the Cold War would prove to be a conflict of “proxy” wars, to include conflicts in Korea, Vietnam, and Afghanistan. In addition to actual combat, both sides engaged in a war of propaganda, in which they hurled rhetoric against each other, attempting to solidify their position with their allies while drawing the favor of nonaligned countries. It was a diplomatic war, where such heralded foreign policy ventures as the Marshall Plan had at their core the goal of strengthening allies to make Communism unattractive to their citizenry. Finally, it was an intelligence war, with both sides spying on each other and conducting covert operations in increasingly aggressive ways. Occasionally, the Cold

War threatened to become “hot,” with events such as the Cuban Missile Crisis. In a very real sense, the Cold War gave birth to the U.S. intelligence infrastructure.

## National Security Act of 1947

After World War II, Congress and the President Truman realized that they could no longer place a low priority on intelligence. At the same time, Truman was concerned that an overly powerful intelligence infrastructure could damage liberty and privacy. He believed that the OSS was too powerful for peacetime and that a civilian agency should be established. He decided instead to appoint a **Director of Central Intelligence (DCI)** to oversee events. As a further step, the Congress passed the **National Security Act of 1947**, an extremely important piece of legislation that created both the CIA and the **National Security Council** and established laws relating to intelligence collection and covert activities. To keep the CIA from becoming too powerful, two very important restrictions were placed upon it: (1) it was not given law enforcement powers and (2) it was mandated to operate primarily outside the United States.

## Early Days of the CIA

By 1947, it was clear that the intent of Communism was to spread its influence around the world. In Italy, Communism was gaining popularity. The western IC worried that the Communists might prevail in the 1948 Italian elections, extending the reach of the “Iron Curtain” to the Mediterranean. To counter this threat, the CIA engaged in one of its first major covert actions, funneling large sums of cash to the opposition party and authoring letters and anticommunist books. The CIA-backed Christian Democrats won, giving the CIA an early Cold War victory (Weiner, 2006).

The success of the Italian operation emboldened American policymakers; another major challenge came in Iran, where the popularly elected Prime Minister, Mohammed Mosaddeq, threatened to nationalize the oil companies inside that country that belonged to Britain. Distraught over this prospect but unable to do anything themselves, the British approached the Truman administration in the hopes that the United States would see this as a way to deter Communism and intervene. Although President Truman was cool to the idea, his successor, Dwight Eisenhower, had no such qualms.

In 1953, Mosaddeq was overthrown in a coup engineered by the CIA in what was termed **Operation Ajax**. His successor, Mohammad Reza Pahlavi, was a member of the Iranian royal family and, understandably, a great fan of the United States. Better known in the West as the Shah of Iran, Pahlavi was a friend to America throughout his reign, which lasted until 1979. However,



he was also an absolute and tyrannical monarch and employed a fearsome secret police force known as the SAVAK. This proved wildly unpopular with many Iranians who did not soon forget the United States' complicity in the overthrow of their democratically elected government. By the late 1970s, the stage was set for yet another coup in Iran. This time, however, the people rose up against the Shah and replaced him with a popular Shiite Muslim cleric, the Grand Ayatollah Ruhollah Mousavi Khomeini, who had been exiled years before. Khomeini shared his countrymen's disdain for the United States, turning a once strong ally into a bitter foe virtually overnight (Kinzer, 2004).

Throughout this period, the CIA was busy confronting Communism throughout the world. As had happened in Iran, the democratically elected President of Guatemala, Jacobo Arbenz Guzmán, contemplated redistributing foreign wealth to his citizens. "Redistribution of wealth" sounded a great deal like Communism to the Eisenhower administration which once again turned to covert action, staging a coup against Guzman in 1954. The operation turned into a farce, with horrendously poor planning and sloppy execution. Nevertheless, it succeeded. By the mid-1950s, it appeared that covert operations were providing America with a significant strategic advantage. However, as future years would demonstrate, these actions could become a double-edged sword; even when they succeeded in the short term, as in Iran, their long-term effects could prove quite damaging (see Cullather, 1999).

## Korean War

Like many other countries, Korea was divided in two after World War II, with a Communist North and a democratic South. This relationship, however, proved difficult. On June 25, 1950, North Korean forces invaded the South in a surprise attack, hoping to unify the country under Communist rule. As it had with Pearl Harbor, the IC missed many signals of an impending invasion and incorrectly concluded that the South would be able to withstand an onslaught from the North.

The United Nations, led by the United States, condemned the attack and committed troops to fight the North. The Korean War, which lasted until 1953, was the first **proxy war** or so called "police action" in which the United States and the Soviet Union indirectly confronted one another; it would not be the last. The conflict, which ended in a stalemate, pointed out significant gaps in U.S. intelligence, which included failures that directly influenced the decision of Communist China to enter the conflict against the United States and the United Nation's forces.

One glaring and obvious conclusion driven home by the events of the war was that the various military intelligence arms did not communicate well with one another. Eventually, in 1961, the Defense Intelligence Agency (DIA) was created. The DIA did not replace the intelligence services of the

armed forces; rather, its mission included collecting, analyzing, and integrating intelligence and advising the Secretary of Defense and Chairman of the Joint Chiefs of Staff in matters pertaining to military intelligence.

## Creation of the National Security Agency

The 1940s and 1950s witnessed significant technological advances in communications. In addition, Project Ultra had convinced the United States of the value of SIGINT. Consequently, in 1949, the military established the Armed Forces Security Agency (AFSA), whose primary mission was to intercept and analyze foreign SIGINT. However, it soon became clear that AFSA was not up to the task; by 1952, it had been replaced by the National Security Agency (NSA), a supersecret organization whose mission was strictly SIGINT. By the end of the Cold War, both SIGINT and imagery intelligence (IMINT) played a huge role in gathering intelligence about the Soviets and their allies. In large part, this had to do with the organizational structure of the Soviet Union. With its large militaries and massive bureaucracies, the Soviets needed to communicate constantly to maintain command and control (SIGINT). As well, the United States could easily count Soviet tanks and ships from the air and could thereby keep a close eye on the military capabilities of its number one adversary (IMINT).

## Evolution of IMINT

As the United States entered the Cold War, it had little in the way of an IMINT capability; the best America could do was to refurbish old bombers and fly them near the Soviet border or into Soviet airspace. President Eisenhower, who had used SIGINT and IMINT extensively as a military commander, was thoroughly dissatisfied with this situation.

To fix the problem, he commissioned the construction of a special plane designed specifically for spying. Dubbed the U-2, the first prototype aircraft flew in 1955. The U-2 was an exceptional plane for its day, flying upward of 70,000 feet and equipped with sophisticated cameras.

Not wishing to provoke a military response in case of an accident, Eisenhower turned the U-2 over to the CIA instead of the military. However, the vast majority of individuals capable of flying such a difficult and sophisticated aircraft were, in fact, Air Force or Navy pilots. To alleviate the problem, military pilots temporarily resigned their commissions and joined the CIA; this was a procedure that became known as “sheep dipping” (Huntington, 2007).

The U-2s began their missions in the mid 1950s, flying directly over the Soviet Union and providing excellent photographs. However, on May 1, 1960, a U-2 piloted by **Francis Gary Powers** was shot down by a missile near



Sverdlovsk in the Soviet Union. This incident provided the Soviet Union with an excellent stage upon which to grab the attention of the world—the United States had been caught spying. The Eisenhower administration belatedly admitted its culpability in the affair, provoking condemnation from the Communist bloc countries.

The U-2 program would continue for several years, during which time it produced much valuable data. Sensing that satellites were the ultimate IMINT platform, the United States began work on the Corona program, which was operational by 1960. At the same time, it developed a sort of space-plane called the SR-71, which flew higher, faster, and further than the U-2.

Today, the term IMINT has been replaced by GEOINT (geospatial intelligence). Both the National Geospatial-Intelligence Agency and the National Reconnaissance Office have responsibility for U.S. satellites, which are responsible for much of the GEOINT gathered today.

## Cuba

In 1956, a Communist revolutionary by the name of Fidel Castro led a group of 82 people in an assault of the island of Cuba, hoping to stage a popular uprising. Against all odds, he succeeded. Cuba is only 90 miles from Florida and the thought of a staunch, dedicated Communist in America's backyard alarmed the Eisenhower administration. Cuba became a focus of the U.S. IC and getting rid of Castro, either by assassination or coup, became a priority.

In 1960, the CIA began training and funding a group of Cuban exiles to invade the island in the hopes of sparking a popular rebellion. In hindsight, the plan was fraught with miscalculations, poor planning, and unwarranted assumptions. For one thing, it was assumed that the Cuban people would back an invading force and rise up against Castro. By the CIA's own admission, it failed to organize sufficient internal resistance; ultimately, the majority of the citizenry sided with Castro. In addition, the Cuban government had learned about the planned invasion and took steps to respond.

On April 15, 1961, a group of American B-26 bombers, flown by exiles and disguised to look like aircraft of the Cuban Air Force, attacked military airfields in Cuba. On April 17, approximately 1300 exiles came ashore on a beach at the mouth of Bahía de Cochinos, or the **Bay of Pigs**.

The invasion soon failed. The initial airstrikes had been largely ineffective; the Kennedy administration, fearful that its hand in the operation would be revealed, canceled subsequent ones. Assisted by the mostly intact Cuban Air Force and thousands of civilian volunteers, the Cuban Army defeated the invaders within three days (Higgins, 1987, 2008).

The Bay of Pigs did not end covert activities against Cuba. In 1961, the President approved Operation Mongoose, a series of secret programs