CHAPTER 5 COLLECTION AND THE COLLECTION DISCIPLINES

COLLECTION IS THE bedrock of intelligence. Intelligence collection has been written about since the biblical references to spies in Numbers, 13–14 and the Book of Joshua. Without collection, intelligence is little more than guesswork—perhaps educated guesswork, but guesswork nonetheless. The United States and several other nations use multiple means of collecting the intelligence they require. The means are driven by two factors: the nature of the intelligence being sought and the ability to acquire it in various ways. In the United States the means of collecting intelligence are sometimes referred to as **collection disciplines** or INTs. This chapter discusses the overarching themes that affect all means of collection, then addresses what the various INTs provide as well as their strengths and weaknesses.

Primarily in the military, collection is sometimes spoken of as ISR: intelligence, surveillance, and reconnaissance. The term covers three different types of activities.

1. Intelligence: a general term for collection
2. Surveillance: the systematic observation of a targeted area or group, usually for an extended period of time
3. Reconnaissance: a mission to acquire information about a target, sometimes meaning a one-time endeavor

OVERARCHING THEMES

Several themes or issues cut across the collection disciplines and tend to drive many of the debates and decisions on intelligence collection. These themes point out that collection involves more than questions like, "What can be collected?" or "Should that be collected?" Collection is a highly complex government activity that requires numerous decisions and has many stress points.

BUDGET. Technical collection systems, many of which are based on satellites, are very expensive. The systems and programs are a major expenditure within the U.S. intelligence budget. Thus, costs always constrain the ability to operate a large number of collection systems at the same time. Moreover, because different types of satellites are employed for different types of collection (imagery versus signals, for example) or may be equipped to carry multiple sensors, policy makers have to make difficult trade-offs. Significant costs are also

associated with launching satellites. The larger the satellite, which is driven in large part by the nature of its sensor package and the equipment needed to power the satellite and to transmit the data, the larger the rocket required to put it into orbit. Finally, the costs of processing and exploitation (P&E), without which collection is meaningless, should be factored into the total expense. Builders of collection systems often ignore P&E and launch costs as part of their estimates for collection.

During the cold war, cost issues for technical collection rarely surfaced. The sense of threat, coupled with the fact that no better way existed to collect intelligence on the Soviet Union, tended to support the high costs of the systems. Also, decision makers placed greater emphasis on collection systems than on the processing and exploitation needed to deal with the intelligence collected. In the immediate post–cold war period, given the absence of any large and potentially overwhelming threat, collection costs became more vulnerable politically. The terrorist attacks in 2001 raised additional questions about the utility of these systems, as terrorist targets are less susceptible to collection via technical means and may require greater use of human intelligence.

There have been several recent decisions that underscore the increased difficulty in sustaining the costs of technical collection. In June 2005, Rep. Peter Hoekstra, R.-Mich., chairman of the House Intelligence Committee, argued that too much money was being spent on satellites and not enough on human collectors and on analysts with language skills. Advocates for both views exist, but this is the sort of argument that rarely would have been made during the cold war. One of director of national intelligence (DNI) John Negroponte's major collection decisions came in September 2005, when he ordered the Boeing Company to stop work on a system known as the Future Imagery Architecture (FIA), widely thought to be the next generation of imagery satellites. FIA had fallen way behind schedule and had also incurred cost overruns. (According to detailed press accounts, FIA had gone from a program bid at $5 billion to more than $18 billion and was still $2 to $3 billion short.) This move was also seen as an attempt by the DNI to have a greater say in satellite decisions, which have customarily been dominated by the Department of Defense (DOD). Two years later, in August 2007, National Reconnaissance Office (NRO) director Donald Kerr testified publicly (during his nomination hearings to be the new principal deputy DNI) that he had recommended terminating two other satellite collection programs because he believed they could not be successfully completed.

An added complication in building future technical collection systems is the shrinking industrial base that occurred in the 1990s. Secretary of Defense William Perry (1994–1997) had urged defense contractors to consolidate, arguing that there were too many firms competing for declining defense dollars. A period of consolidation followed, with firms either merging or acquiring one another. In the late 1990s it became apparent that there were now actually very few firms left, especially in such high specialty areas as technical collection systems. Thus, in the case of FIA there were only two industrial teams bidding on the contract.

The intelligence budget is also important because it is a major means by which Congress influences and even controls intelligence activities. Congress tended to be supportive of collection requirements throughout the cold war, but it was also inclined to support the disparity between collection and the less-favored processing and exploitation. Some changes in emphasis began to appear in the mid-1990s. The House Intelligence Committee, for example, advocated the use of some smaller imagery satellites, both to have greater flexibility and to save on building and launching costs. This committee also tried to redress the collection and P&E balance, emphasizing the importance of TPEDs (tasking, processing, exploitation, and dissemination). However, the TPEDs problem remains and may grow worse as new collection systems are launched, as they will have increased collection capabilities. Indeed, it has become increasingly difficult to get congressional backing for new collection systems without promising to improve the amount of intelligence that is processed and exploited.

LONG LEAD TIMES. All technical collection systems are extremely complex. They have to be able to collect the desired data, perhaps store it, and then send it to a remote location where it can be processed. All systems have to be rugged enough to endure difficult conditions, whether Earth-bound or space-based, although those in space face more austere challenges. No matter how satisfactory current collection capabilities are, there are several impetuses to build new systems: to improve collection capabilities, to take advantage of new technologies, and to respond to changing intelligence priorities.

The technological challenges alone are daunting and are a significant factor in the time required to build and launch a new system. From the point that a decision is made to acquire such new technology to the actual launch can be as long as ten to fifteen years. Reaching the decision to build a new system involves additional time (sometimes several years) as intelligence agencies and their policy customers debate which intelligence needs should take priority, which technologies should be pursued, and what trade-offs should be made among competing systems in an always constrained budget. Getting congressional approval can also take several years, especially if there is disagreement on which systems should have funding priority. DNI Mike McConnell has expressed his frustration with the satellite acquisition system, comparing the U.S. system with that of Europe, where a satellite can be developed in five years and cost less than $1 billion. But McConnell also admits that U.S. satellites are built to collect against a more diverse set of targets and that there is now a higher degree of risk aversion prevalent in the U.S. system. This last point is important. Collection satellites are extremely complex to build, orbit, and manage, and launching them into a proper orbit really is rocket science. It is interesting to contrast the risk-averse atmosphere that DNI McConnell notes with the early history of U.S. intelligence satellites. According to the NRO, there were twelve CORONA satellite launches in 1959–1960 before the first successful recovery and thirteen before the first image taken in space.

The net result of the lead times involved (not even taking into account the decision time) is that, when a system is launched, its technology may be dated and a whole new set of intelligence priorities may have emerged that the system was not designed to address. There are

no shortcuts in system development if a commitment has been made to improving capabilities on a regular basis, which remains the best choice.

COLLECTION SYNERGY. One of the major advantages of having multiple means of collection is that one system or discipline can provide tips or clues that can be used to guide collection by other systems. For major requirements, more than one type of collection is used; the collectors are designed to be cooperative when the system is working correctly. The goal of the U.S. intelligence community is to produce **all-source intelligence,** or fusion intelligence—in other words, intelligence based on as many collection sources as possible to compensate for the shortcomings of each and to profit from their combined strength. Under the 2004 IRTPA, the DNI is responsible for ensuring that "finished intelligence [is] based upon all sources of available intelligence." This is a somewhat odd provision, akin to a DNI collection seal of approval. It is also ambiguous, as it can be interpreted to mean all sources that should be brought to bear on an issue or all the sources that are available, taking into account other priorities as well. All-source intelligence reflects collection in depth. At the same time, the diverse array allows collection managers to increase collection in breadth, that is, to increase the number of issues being covered, albeit with less depth for a particular issue.

An excellent example of collection synergy is the Cuban Missile Crisis of 1962. Although analysts were slow to understand that Soviet premier Nikita Khrushchev was willing to make such a risky move as deploying medium- and intermediate-range missiles in Cuba, the intelligence community brought a variety of collection means to bear. Anti–Fidel Castro Cubans still on the island provided some of the first reliable evidence that missiles were being deployed. A human source provided the data that targeted the U-2 flights over a trapezoid-shaped area bounded by four towns in western Cuba. Imagery then provided crucial intelligence about the status of the missile sites and the approximate time before completion, as did Soviet technical manuals turned over to the United States by Soviet colonel Oleg Penkovsky, a spy in the employ of the United States and Britain. Imagery and naval units gave the locations of Soviet ships bringing the missiles to the almost-completed sites. Finally, Penkovsky provided the United States with excellent authoritative information on the state of Soviet strategic forces, which indicated overwhelming U.S. superiority.

THE VACUUM CLEANER PROBLEM. Those familiar with U.S. technical collection systems often note that they have more in common with vacuum cleaners than they do with microscopes. In other words, collectors sweep up a great deal of information, within which may be the intelligence being sought. This problem is sometimes also referred to as **wheat versus chaff.** Roberta Wohlstetter, in her classic study *Pearl Harbor: Warning and Decision,* refers to the problem as **noise versus signals,** noting that the signals one wishes to receive and to know are often embedded in a great deal of surrounding noise.

No matter which metaphor one uses, the issue is the same: Technical collection is less than precise. The problem underscores the importance of processing and exploitation.

The issue then becomes how to extract the desired intelligence from the mountain of information. One answer would be to increase the number of analysts who deal with the incoming intelligence, but that raises additional demands on the budget. Another possible response, even less palatable, would be to collect less. But, even then, there would be no assurance that the "wheat" could be found within the smaller volume being collected.

THE PROCESSING AND EXPLOITATION IMBALANCE. A large imbalance exists between the amount of images or signals that are collected and the amount that are processed and exploited. This reflects, in part, the sheer amount that is collected. It also reflects years of budget choices by the intelligence community and Congress that have favored new collection systems over improving P&E capabilities. According to DOD, for example, the National Security Agency (NSA) records 650 million events daily, which culminates in ten thousand reports. Although methodologies are in place to ensure that the most important intelligence is processed and exploited, an important image or message could be overlooked. DOD considered posting all collected intelligence in a single repository and then processing those items selected by analysts. This would, in theory, ensure that only the intelligence that was needed would be processed and analyzed, but it would also increase the burden on analysts to find the intelligence they needed instead of having it sent to them. The Central Intelligence Agency (CIA) is evaluating technology that would automatically examine digital images or video clips to look for details (such as a car) that are the same as those stored in an imagery library. Neither of these suggestions gets at the central issue—that P&E requires more manpower and more funding if it is to have a better chance of getting the necessary intelligence out of the vast amount of information that is collected.

The P&E imbalance has become a political issue when Congress makes budget decisions. As noted, the intelligence committees find it difficult to put money into new collection systems when they are told that only as many images or signals will be processed and exploited as was the case for the previous generations of collectors. Although there may be valid explanations for this outcome, Congress—as might be imagined—would rather see increasingly expensive systems result in more collected intelligence that can be used by analysts.

COMPETING COLLECTION PRIORITIES. Given that the number of collection platforms, or **spies,** is limited, policy makers must make choices among competing collection requirements. They use various systems to set priorities, but some issues inevitably get shorter shrift, or may be ignored altogether, in favor of those that are seen as more pressing.

Both policy makers and the intelligence officers acting on their behalf request increased collection on certain issues. However, their requests are made within a system that is inelastic in terms of both technical and human collectors. Every collection request that is fulfilled means another collection issue or request goes wanting; it is a zero-sum game. That is why a priority system is necessary in the first place. Moreover, the system has little or no surge capacity; few collection systems (airplanes, drones, and ship-based systems) or spies are

waiting in reserve for an emergency. Even if additional satellites have already been built, launching them requires a ready rocket of the appropriate size, an available launch pad, and other resources. (The Soviet Union used a different collection model. Soviet satellites lacked the life spans of their U.S. counterparts. During crises, the Soviets supplemented current collection assets with additional, usually short-lived, satellites, which were kept on hand with launch vehicles ready.) Similarly, one does not simply tap a spy and send him or her off to a new assignment. Cover stories need to be created, along with the inevitable paraphernalia; training may be necessary; and a host of other preparations must be made. Inelasticity of resources makes the priorities system difficult at best.

The shifting—or nonshifting—of collection resources in the face of novel situations or emergencies is always subject to 20/20 hindsight. For example, in May 1998 the newly elected government of India resumed testing nuclear weapons, as it had promised in its election campaign. The U.S. intelligence community had not detected the test preparations. As a result, Director of Central Intelligence (DCI) George J. Tenet (1997–2004) asked retired admiral David Jeremiah to review the intelligence community's performance on this hard-target issue—preventing the proliferation of nuclear weapons.

Jeremiah reported several findings, including the fact that—given the Indian government's avowed intention to test, which required no clandestine collection to learn—intelligence performance could have been better. But he noted that collection assets that might have picked up indications of the impending test were focused on the Korean demilitarized zone (DMZ), at the request of the commander of U.S. forces in Korea. As an NSA director put it, the Korean DMZ was the only place in the world in the late 1990s where someone else could decide if the United States would go to war. Although the Korean DMZ remains a constant concern, for a brief period in 1998, Indian test activities perhaps should have been accorded a higher priority.

COLLECTION SWARM BALL. A major problem that has occurred in managing collection is the phenomenon known as collection **swarm ball**. This refers to the tendency of all collectors or collection agencies to collect on an issue that is deemed to be important, whether or not they bring anything useful to the table or can offer an appropriate type of collection. It is called "swarm ball" because it resembles the tactics of small children playing soccer, in which both teams converge on the ball en masse regardless of their assigned positions. Swarm ball has usually involved high-priority issues. For example, if a high-priority issue was the cyber attack capabilities of a hostile state, little value would be gained by imagery, although imagery collection managers might be tempted to contribute to the issue based solely on its priority. The impetus for swarm ball is clear: It allows collectors to show that they are working on high-value issues, regardless of their contribution, which will be important for their continued support in the next round of budget allocations.

The solution to swarm ball is twofold. First, agreement must be reached on which INTs are responsible for collecting on specific issues or priorities. This is not a difficult agreement to reach, although it is time consuming, as the attributes of most issues can be delineated (locations, facilities, people involved, likelihood of communications, types of intelligence that is needed, and so on) and then matched against current or impending collection capabilities. Second, the agreement must be rigorously enforced, and agencies must not be penalized for not collecting against issues not suited to them regardless of the issues' importance and must be recognized for concentrating on the issues about which they can collect needed intelligence.

PROTECTING SOURCES AND METHODS. The details of collection capabilities—and even the existence of some capabilities—are among the most highly classified secrets of any state. In U.S. parlance, classification is referred to as the protection of **sources and methods.** It is one of the primary concerns of the entire intelligence community and a task specifically assigned by law to the director of national intelligence.

Several levels of classification are in use, reflecting the sensitivity of the intelligence or intelligence means. *(See box, "Why Classify?")* The security classifications are driven by concerns that the disclosure of capabilities will allow those nations that are collection targets to take steps to prevent collection, thus effectively negating the collection systems. However, the levels of classification also impose costs, some of which are financial. The physical costs of security—guards, safes, and special means of transmitting intelligence—are high. Added to these is the expense of security checks for individuals who are to be entrusted with classified information (see chap. 7 for details).

Critics maintain that the classification system is sometimes used inappropriately and even promiscuously, classifying material too highly or, in some cases, classifying material that does not deserve to be classified. Critics are also concerned that the system can be abused to allow the intelligence community to hide mistakes, failures, or even crimes.

Beyond the costs of the classification system and its potential abuse, the need to conceal sources and methods limits the use of intelligence as a policy tool. For example, in the late 1950s Khrushchev broke a nuclear test moratorium and blustered about the Soviet Union's growing strategic nuclear forces. President Dwight D. Eisenhower, bolstered by the first images of the Soviet strategic forces, knew that the United States enjoyed a strong strategic superiority. But, to protect sources and methods, Eisenhower did not reply to Khrushchev's false boasts. What might have been the results if the United States had released some imagery to counter the Soviet claims? Would the release have spurred the Soviets to greater weapons-building efforts? Would it have severely undercut Soviet foreign policy? Would it have affected U.S. intelligence capabilities, even though the Soviets already knew their country was being overflown by U-2s and later by satellites? These questions are not answerable, but they provide a good overview on the problem.

More recently, the U.S. intelligence community has grown concerned about protecting intelligence sources and methods during post–cold war military operations that involve cooperation with nations that are not U.S. allies. Even among allies the United States

WHY CLASSIFY?

Numerous critics of the U.S. classification system have argued—not incorrectly—that classification is used too freely and sometimes for the sake of denying information to others who have a legitimate need for it.

However, a rationale and some sense are behind the way in which classification is intended to be used. Classification derives from the damage that would be done if the information were revealed. Thus, classification related to intelligence collection underscores both the importance of the information and the fragility of its source—something that would be difficult to replace if disclosed.

The most common classification is SECRET (CONFIDENTIAL is rarely used any longer), followed by TOP SECRET. Within TOP SECRET are numerous TOP SECRET/CODEWORD compartments—meaning specific bodies of intelligence based on their sources. Admission to any level of classification or compartment is driven by an individual's certified need to know that specific type of information.

Each classification level is defined; current definitions are found in Executive Order 13292 of March 25, 2003.

- CONFIDENTIAL: information whose unauthorized disclosure "could be expected to cause damage to the national security."
- SECRET: information whose unauthorized disclosure "could be expected to cause serious damage to the national security."
- TOP SECRET: information whose unauthorized disclosure "could be expected to cause exceptionally grave damage to the national security."

Higher levels of access are useful bureaucratic levers for those who have them in contrast to those who do not.

employs gradations of intelligence sharing, having the deepest such relationship with Britain, followed closely by Australia and Canada. Intelligence relations with other North Atlantic Treaty Organization (NATO) allies are close, albeit less so than with the "Commonwealth cousins." But some operations, such as in Bosnia, have involved military operations with nations that are viewed with lingering suspicion, such as Russia and Ukraine. In these cases the need to protect intelligence sources and methods must be balanced against the need to share intelligence—not only for the sake of the operation but also to ensure that military partners in the operation are not put in a position in which their actions or inactions prove to be dangerous to U.S. troops.

Another intelligence sharing issue arose in 2002–2003, in the months before Operation Iraqi Freedom. The United States and Britain said they would provide intelligence on Iraqi WMD to United Nations (UN) inspectors but not necessarily all available intelligence. Some controversy arose after DCI Tenet said the United States was cooperating fully but the CIA later revealed that it had shared intelligence on 84 of 105 suspected priority weapons sites, which some members of Congress felt was not what they had understood to be the agreed level of intelligence sharing.

LIMITATIONS OF SATELLITES. All satellites are limited by the laws of physics. Most orbiting systems can spend only a limited time over any target. On each successive orbit the satellites shift to a slightly different coverage pattern. (Satellites correspond to the motion of the earth, as they are trapped within Earth's gravitational pull. Thus, satellites' orbits move from west to east with each pass.) Moreover, satellites travel in predictable orbits. Potential targets of a satellite can derive the orbit from basic knowledge about its launch and initial orbit. For a variety of reasons, some individuals and organizations attempt to publicize this information. This enables nations to take steps to avoid collection—in part by engaging in activities they wish to keep secret only when satellites are not overhead.

Satellites that are in **geosynchronous orbit** stay over the same spot on Earth at all times. But to do this they must be placed twenty-two thousand miles above Earth. The great distance between the collectors and their targets raises the problem of transmitting collected information back to Earth. Collection can be precise only up to a point, thus explaining the vacuum cleaner problem. Satellites can also be flown in **sun-synchronous orbits,** that is, moving in harmony with the Earth's rotation so as to always remain where there is daylight, but this produces an easily tracked orbit. Sun-synchronous orbit is better for commercial satellites than for national imagery satellites.

Another interesting orbit is the "Molniya" orbit, named after the Soviet communications satellites that first used them. The Molniya orbit is highly elliptical, coming close to the Earth over the southern hemisphere (perhaps 300 miles) and then much further away from the Earth over the northern hemisphere (perhaps 25,000 miles). In this pattern, a satellite revolves around the Earth twice in a day. It is important to remember that the Earth's land mass is not evenly distributed; much more of it lies north of the equator than south of it. The advantage of the Molniya orbit is that it moves very quickly across the southern hemisphere, where there are likely to be fewer targets, because it is close to the Earth's gravitational pull, but then "lingers" as it moves across the northern hemisphere when it is further away. Approximately eight of the twelve hours of one revolution will be spent over the northern hemisphere. This allows increased collection over the larger area of land. But the satellite's greater distance over the northern hemisphere also dictates that it does broad area collection as opposed to close-in or "spot" collection.

THE STOVEPIPES PROBLEM. Intelligence practitioners often talk about collection "stovepipes." This term is applied to two characteristics of intelligence collection. First, all of the technical collection disciplines—geospatial intelligence (GEOINT, formerly imagery or IMINT), signals intelligence (SIGINT), and measurement and signatures intelligence (MASINT)—and the nontechnical human intelligence (HUMINT), or **espionage,** have end-to-end processes, from collection through dissemination. (Open-source intelligence—OSINT—should have end-to-end processes, but it does not.) Thus, a pipeline forms from beginning to end. Second, the collection disciplines are separate from one another and are often competitors. The INTs sometimes vie with one another to respond to requests for intelligence—largely as a means of ensuring continuing funding levels—regardless of which

INT is best suited to provide the required intelligence. Often, several INTs respond, regardless of their applicability to the problem, thus creating the swarm ball. Within the U.S. intelligence system, a variety of positions and fora have been designed to coordinate the INTs, but no single individual exercises ultimate control over all of them. During testimony about the 2004 intelligence legislation, some of the tension between the DCI and DOD over control of the National Geospatial-Intelligence Agency (NGA) and NSA was evident. These agencies are, as the names indicate, national intelligence agencies and come under the DNI (or the DCI at the time of the hearings). But NGA and NSA are also DOD agencies and are designated as combat support agencies, thus indicating a degree of control by the secretary of defense as well. The legislation creating the DNI does not clarify this situation. The stovepipes are therefore complete but individual and separate processes.

Intelligence officers also sometimes talk about the "stovepipes within the stovepipes." Within specific collection disciplines, separate programs and processes likely work somewhat independently of one another and do not have insights into one another's operations, but they have an aggregate competitive effect that influences a particular INT. This is, in part, the natural result of the compartmentation of various programs for the sake of security, but it further exacerbates the stovepipes issue and makes cross-INT strategies more difficult.

THE OPACITY OF INTELLIGENCE. The U.S. intelligence process seeks to have analysis-driven collection. This is a shorthand way of recognizing that collection priorities should reflect the intelligence needs of those crafting the analysis. It further reflects the expectation, occasionally misplaced, that analysts have received a sense of the priorities from policy makers. In reality, the collection and analytical communities do not operate as closely as some expect. One of the most striking aspects of this is the view held by many analysts, including veteran ones, that the collection system is a black box into which analysts have little insight. Analysts say that they have no real sense of how collection-tasking decisions are made, what gets collected for which reasons, or how they receive their intelligence. To many analysts, the collection process is something of a mystery. This could simply be dismissed as the failure of one professional group to understand the methods of another group. But the divide goes to the heart of collection, often leaving analysts believing that they have no influence on collection and that whatever sources they do get are somewhat random and fortuitous. This view is significant because the intelligence community does spend some time educating analysts about collection, but often with little apparent return on the investment. This perceived opacity of collection also undercuts the goal of having analysis drive collection. It is difficult to know how to task a system that one does not fully understand.

DNI McConnell has taken some steps to improve the collection-analysis liaison. The current most pressing and difficult intelligence issues (Iran, North Korea, Cuba/Venezuela, terrorism, WMD proliferation, counterintelligence) have been assigned to mission managers, at the recommendation of the WMD Commission. These mission managers report to both the deputy DNIs for analysis and collection and are responsible for ensuring that the two aspects of intelligence work together to improve both collection and analysis. This arrangement likely improves coordination at the top but does not solve the problem of too many analysts not having a complete or useful understanding of the collection system.

DENIAL AND DECEPTION. A targeted nation can use knowledge about the collection capabilities of an opponent to avoid collection (known as **denial**); the target can use the same knowledge to transmit information to a collector. This information can be true or false; if the latter, it is called **deception.** For example, a nation can display an array of weapons as a means of deterring attack. Such a display may reveal actual capabilities or may be staged to present a false image of strength. A classic example was when the Soviet Union sent its limited number of strategic bombers in large loops around Moscow during parades so they could be repeatedly counted by U.S. personnel in attendance, thus inflating Soviet air strength. The use of decoys or dummies to fool imagery, or false communications to fool SIGINT, also falls into this category. In World War II, the Allies exploited these techniques prior to D-Day to raise German concerns about an invasion in the Pas de Calais instead of Normandy. The Allies created a nonexistent invasion force, replete with inflatable dummy tanks and streams of false radio traffic, all under the supposed command of Gen. George S. Patton. In August 2006, the British Ordnance Survey, which is responsible for all official British maps (and traces its heritage back to 1791), announced that it would end an 80-year program of falsifying maps. During World War II, sensitive sites had been deleted from official maps to thwart German bombing targets. The British government noted that this deception policy had been made obsolete by high resolution satellite imagery and sources available on the Internet.

The intelligence community has devoted ever-increasing resources to the issue of denial and deception, also known as D&D. Intelligence officials seek to know which nations are practicing D&D, determine how they may have obtained the intelligence that made D&D possible, and then seek to design countermeasures to circumvent D&D. As more information about U.S. intelligence sources and methods becomes publicly available, D&D is an increasing constraint on U.S. collection.

However, D&D is also a complex analytical issue and must be approached carefully. Assume, for example, that a potentially hostile state, which has practiced D&D, is believed to be fielding a new weapons system. Collectors are tasked to find it, if possible, but they cannot. Why? Is it a case of D&D or is there no system to find? One cannot simply assume that failed collection is a result of D&D. The completely innocent state and the state with very good D&D both look identical to the observer. Thus, within D&D analysis lies the potential pitfall of self-deception. (One intelligence community wag put it this way: "We have never discovered a successful deception activity.")

RECONNAISSANCE IN THE POST–COLD WAR WORLD. The U.S. intelligence collection array was largely built to respond to the difficulties of penetrating the Soviet target, a closed

society with a vast land mass, frequent bad weather, and a long-standing tradition of secrecy and deception. At the same time, the primary targets of interest—military capabilities—existed in extensive and well-defined bases with a large supporting infrastructure and exercised with great regularity, thus alleviating the problem to some extent.

Does the United States require the same extensive array of collection systems to deal with post–cold war intelligence issues? On the one hand, the threat to the United States has lessened. On the other hand, intelligence targets are more diffuse and more geographically disparate than before. Also, some of the leading intelligence issues—the so-called transnational issues such as narcotics, terrorism, and crime—may be less susceptible to the technical collection capabilities built to deal with the Soviet Union or other classic political-military intelligence problems. Many of the current collection targets are nonstate actors with no fixed geographic location and no vast infrastructure that offers collection opportunities. These transnational issues may require greater human intelligence, albeit in geographic regions where the United States has fewer capabilities. At the same time, nation-state problems remain in North Korea, Iran, Russia, and China. Thus, it does not make sense to abandon entirely the old method of collection, and doing so would be fiscally impractical as well.

Commercial overhead imagery capabilities can be used to augment national systems. Systems such as *IKONOS, LANDSAT, SPOT,* a have ended the U.S. and Russian monopoly on overhead imagery. Any nation—or transnational group—can order imagery from commercial vendors. They may even do so through false fronts to mask their identity. This commercial capability remains so new that its implications have not been completely thought out by those building the commercial systems and by intelligence agencies. On the positive side, commercial imagery offers opportunities, freeing classified collection systems for the truly hard targets.

In 2007, Lt. Gen. David Deptula, the senior intelligence officer in the U.S. Air Force, noted that commercial imagery and online mapping software allowed anyone detailed knowledge of potential targets. Deptula also acknowledged that this capability could not be controlled or reversed. A sense of the power of these commercially available capabilities can be had from the August 2007 announcement by Digital Globe, a U.S. commercial system, prior to the launch of its WorldView-1 satellite. This satellite will be able to revisit a site every 1.7 days and will be capable of taking images of up 290,000 square miles (750,000 sq. km) a day, with a resolution (see below) of 0.5 meters (roughly 20 in.). Interestingly, WorldView was developed in cooperation with NGA to ensure continued access to high quality commercial imagery. **Shutter control** (that is, who controls what the satellites will photograph) is already an issue, for example, between those in the U.S. government who seek to limit photography of Israel and those who own the satellites. Dramatic changes occurred in the U.S. use of commercial imagery during the Afghanistan campaign (2001–), affecting each of these issues and perhaps suggesting a new relationship between the intelligence community and these commercial providers.

Finally, open-source information is growing rapidly. The collapse of a number of closed, Soviet-dominated societies drastically reduced the **denied targets** area, that is, target areas

to which one does not have ready access. One intelligence veteran observed that during the cold war 80 percent of the information about the Soviet Union was secret and 20 percent was open, but in the post–cold war period the ratio had more than reversed for Russia. Theoretically, the greater availability of open-source intelligence should make the intelligence community's job easier. However, this community was created to collect secrets; collecting open-source information is not a wholly analogous activity. The intelligence community has had difficulties assimilating open-source information into its collection stream. Moreover, the intelligence community harbors some institutional prejudice against open-source intelligence, as it seems to run counter to the purposes for which the intelligence community was created.

SATELLITE VULNERABILITY. As much as technical collection satellites are national assets, they also represent points of vulnerability. During the cold war, the United States and the Soviet Union both considered deploying **antisatellite** (ASAT) weapons, and both nations tested ASATs. There were efforts to negotiate a specific ASAT arms control treaty but these did not prove productive. However, in a series of treaties limiting or reducing strategic nuclear weapons [the strategic arms limitation talks (SALT) agreement, Antiballistic Missile (ABM) Treaty, SALT I and II Treaties, and the Strategic Arms Reduction Treaty (START)] both nations agreed not to interfere with one another's "national technical means" of collection (NTMs), a euphemism for the satellites. Both nations appeared to agree that strategic stability depended on knowing what the other state was doing, rather than operating blindly in a crisis.

In the period after the collapse of the Soviet Union there were frequent press reports that an apparently impoverished Russia had, at best, only a few operational imagery satellites. Some reports suggested that, for periods of time, the Russians were "blind." This could be seen as dangerous not only by Russia but by other states as well, again fearing miscalculations during a crisis.

The United States is extremely dependent on satellites for intelligence collection, for communications, and for a host of commercial applications. Much of the U.S. military advantage, the Revolution in Military Affairs (RMA), depends on accurate, timely intelligence being fed to U.S. forces on a continuous basis. Although no state is likely to be able to compete with the United States militarily for some time to come, U.S. forces could be hobbled by attacks on satellite systems. That is why the Chinese ASAT test on January 11, 2007, in which they destroyed an old weather satellite, raised concerns in the United States and among U.S. allies. According to press accounts, U.S. intelligence had discovered indications of the ASAT preparations but the Bush administration chose not to say anything until after the test, although it is not clear that a U.S. intervention would have led to the test's cancellation. There have also been press reports alleging that China has fired lasers in an effort to disable U.S. satellites when they pass over China.

There are few available remedies to a hostile ASAT capability. There are no alternatives to the roles played by satellites. Hardening satellites to enable them to withstand attack is

difficult and makes them that much heavier, requiring a trade-off against collection payloads. It would be possible to build additional reserve satellites that could be launched if existing ones were disabled, but this requires an additional large investment. Even with additional satellites, there would be periods in which the lost capability could not be replaced immediately if weather or technical issues delayed a launch—again assuming that the reserve satellites were loaded on a rocket and placed on a launch pad, ready to go (an eventuality that raises maintenance and reliability questions). The U.S. Air Force is looking at the possible creation of minisatellites that could navigate autonomously and be used to inspect satellites or spacecraft for damage. This program could be useful in the event of an ASAT attack or presumed ASAT attack. Critics have argued that these satellites could also be used to disable hostile satellites.

Some might argue that an ASAT attack would be an act of war. However, even if one were able to determine who had conducted the ASAT attack, the attack itself would limit the ability to command, control, and target a military retaliation.

STRENGTHS AND WEAKNESSES

Each of the collection disciplines has strengths and weaknesses. But when evaluating them—especially the weaknesses—it is important to remember that the goal of intelligence is to involve as many collection disciplines as possible on the major issues. This should allow the collectors to gain advantages from mutual reinforcement and from individual capabilities that can compensate for shortcomings in the others.

GEOSPATIAL INTELLIGENCE. GEOINT is a collection discipline that used to be called imagery or IMINT, also referred to as PHOTINT (photo intelligence). It is a direct descendant of the brief practice of sending soldiers up in balloons during the U.S. Civil War (1861–1865). In World War I (1914–1918) and World War II (1939–1945), both sides used airplanes to obtain photos. Airplanes are still employed, but several nations now use imagery satellites. NGA (which until 2003 was the National Imagery and Mapping Agency, NIMA) has overall responsibility for GEOINT, including processing and exploitation. Some imagery also comes via DOD's airborne systems, such as unmanned aerial vehicles (UAVs), or drones. Handheld cameras also are considered part of imagery collection.

NGA defines GEOINT as "information about any object—natural or man-made—that can be observed or referenced to the Earth, and has national security implications." For example, an image of a city includes natural objects (rivers, lakes, and so on) and man-made objects (buildings, roads, bridges, and so on) and can have overlaid on it utility lines, transport lines, and so on. It may also include terrain or geodetic data. Thus, a more complete picture is drawn that may be of greater intelligence value.

The term *imagery* is somewhat misleading in that it is generally considered to be a picture produced by an optical system akin to a camera. Some imagery is produced by optical systems, usually referred to as electro-optical (EO) systems. Early satellites contained film

that was jettisoned in capsules and subsequently recovered and developed. Modern satellites transmit their images as signals, or digital data streams, that are received and reconstructed as images. Radar imagery sends out pulses of radio waves that reflect back to the sensor in varying degrees of brightness, depending on the amount of reflected energy. Radar is thus not dependent on light and therefore can be used in bad weather or at night.

Infrared imagery (IR) produces an image based on the heat reflected by the surfaces being recorded. IR provides the ability to detect warm objects (for example, engines on tanks or planes inside hangars). Some systems, referred to as multispectral or hyperspectral imagery (MSI and HSI, respectively), derive images from spectral analysis. These images are not photographic per se but are built by reflections from several bands across the spectrum of light, some visible, some invisible. They are usually referred to as MASINT.

The level of detail provided by imagery is called **resolution.** Resolution refers to the smallest object that can be distinguished in an image, expressed in size. Designers of imagery systems must make a trade-off between the resolution and the size of the scene being imaged. The better the resolution, the smaller the scene. The degree of resolution that analysts desire depends on the nature of the target and the type of intelligence that is being sought. For example, one-meter resolution allows fairly detailed analysis of man-made objects or subtle changes to terrain. Ten-meter resolution loses some detail but allows the identification of buildings by type or the surveillance of large installations and associated activity. Twenty- to thirty-meter resolution covers a much larger area but allows the identification of large complexes such as airports, factories, and bases. Thus, the degree of resolution has to be appropriate to the analyst's need. Sometimes high resolution is the correct choice; sometimes it is not.

During the cold war it was often popular to refer to the ability to "read the license plates in the Kremlin parking lot"—a wholly irrelevant parameter. Different collection needs have different resolution requirements. For example, keeping track of large-scale troop deployments requires much less detail than tracking the shipment of military weapons. The U.S. intelligence community developed the science of crateology, by which analysts were able to track Soviet arms shipments based on the size and shape of crates being loaded or unloaded from Soviet-bloc cargo vessels. (This analytical practice was subject to deception simply by purposely using misleadingly sized crates to mask the nature of the shipments.)

Several press accounts say that U.S. satellites now have resolutions of ten inches. Commercial imagery is available at a resolution of 0.5 meter (or just under twenty inches), meaning that an object half a meter in size can be distinguished in an image. (By agreement with the U.S. government, U.S. commercial vendors are subject to a twenty-four-hour delay from the time of collection before they can release any imagery with a resolution better than 0.82 meter, or just over thirty-two inches.)

Imagery offers a number of advantages over other collection means. First, it is sometimes graphic and compelling. When shown to policy makers, an easily interpreted image can be worth the proverbial thousand words. Second, imagery is easily understood much

of the time by policy makers. Even though few of them, if any, are trained imagery analysts, all are accustomed to seeing and interpreting images. From family photos to newspapers, magazines, and news broadcasts, policy makers, like many people, spend a considerable part of their day not only looking at images but also interpreting them. Imagery is also easy to use with policy makers in that little or no interpretation is necessary to determine how it was acquired. Although the method by which images are taken from space, transmitted to Earth, and processed is more complex than using a digital camera, policy clients are sufficiently informed to trust the technology and take it for granted.

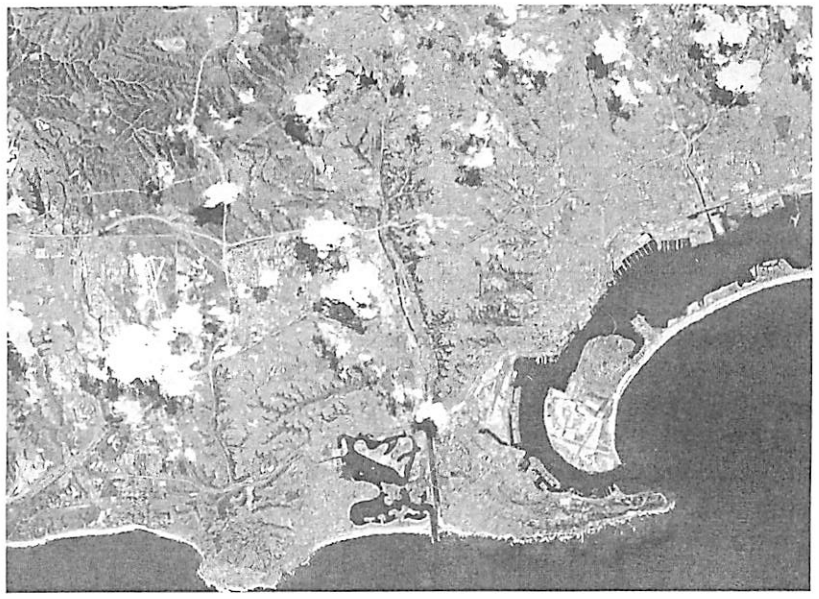
Another advantage of imagery is that many of the targets make themselves available. Military exercises in most nations are conducted on regular cycles and at predictable locations, making them highly susceptible to IMINT. Finally, an image of a certain site often provides information not just about one activity but some ancillary ones as well. A distinction must be made, though, between these military targets, which are familiar to the intelligence community, and the challenges posed by terrorism. In brief, terrorism presents a smaller imagery target. Although training camps may have been set up, as was the case of al Qaeda in Afghanistan, terrorist cells or networks are far smaller, less elaborate, and have less visible infrastructure than do the traditional political-military targets.

Imagery also suffers from a number of problems. The graphic quality that is an advantage can also be a disadvantage. An image can be too compelling, leading to hasty or ill-formed decisions or to the exclusion of other, more subtle intelligence that is contradictory. Also, the intelligence on an image may not be self-evident; it may require interpretation by trained photo interpreters who can see things that the untrained person cannot. At times, the policy makers must take it on faith that the skilled analysts are correct. *(See box, "The Need for Photo Interpreters.")*

Another disadvantage of imagery is that it is only a snapshot, a picture of a particular place at a particular time. This is sometimes referred to as the "where and when" phenomenon. Imagery is a static piece of intelligence, revealing something about where and when it was taken but nothing about what happened before or after or why it happened. Analysts perform a **negation search,** looking at past imagery to determine when an activity commenced. This can be done by computers comparing images, in a process called **automatic change extraction.** The site can be revisited to watch for further activity. But a single image does not reveal everything.

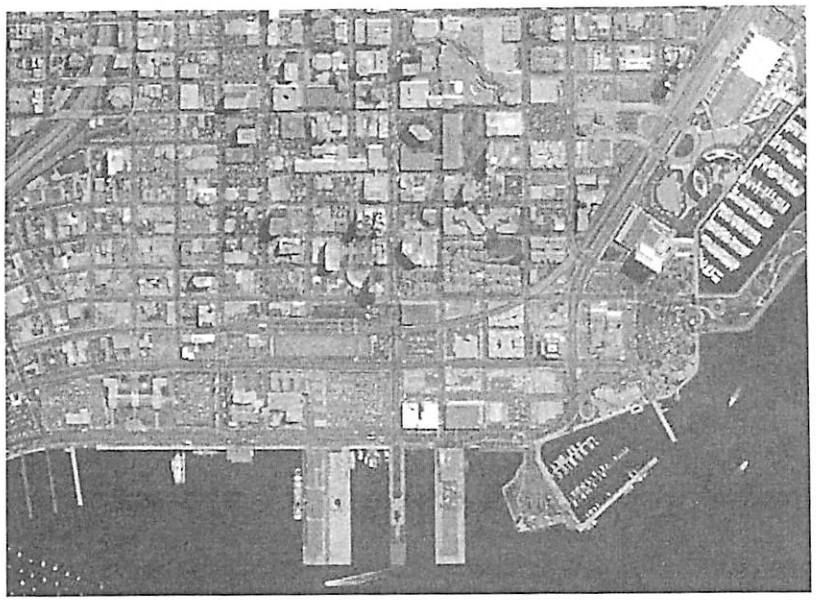
Because details about U.S. imagery capabilities have become better known, states can take steps to deceive collection—through the use of camouflage or dummies—or to preclude collection by conducting certain activities at times when they are unlikely or less likely to be observed.

The war against terrorism led to two major developments in the use of imagery. First, the government greatly expanded its use of commercial imagery. In October 2001, NGA (then known as the NIMA) bought exclusive and perpetual rights to all imagery of Afghanistan taken by the *IKONOS* satellite, operated by the Space Imaging Company. This satellite has a resolution of 0.8 meter (approximately 31.5 inches). The agency's actions

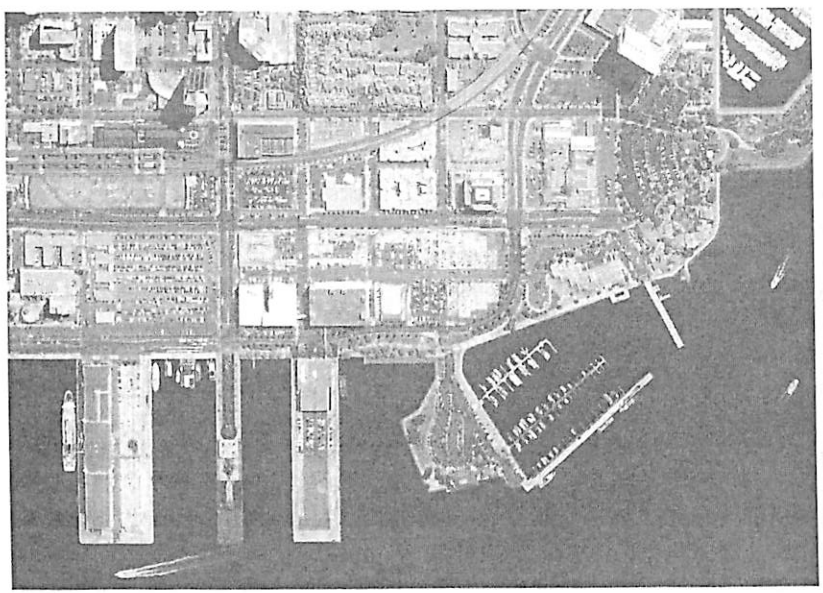


These satellite photos of San Diego, California, illustrate differences in resolution. (Resolution numbers indicate the size of the smallest identifiable object.) They also show recent advances in commercial satellite imagery. The top photo has 25-meter (75 feet) resolution; major landforms—the hills and Mission Bay—are identifiable at lower center. Larger man-made objects—piers, highways, runways at North Island U.S. Naval Air Station—can be seen on the peninsula to the right.

At 5-meter (15 feet) resolution, clarity improves dramatically. North Island and San Diego International Airport are visible, as are rows of boats in the marinas and wakes of boats in the bay. Taller buildings in downtown San Diego can be seen at upper center. Shadows indicate this image was taken in mid- to late morning.



At 4-meter resolution (12 feet), individual buildings and streets can be seen, along with each boat in the marinas. At the bottom, a cruise ship is docked at the terminal. Individual cars can be seen in the parking lot above the piers.



At 1-meter (39 inch) resolution, each building stands out. Individual cars are seen in parking lots and streets. Railroad tracks are visible on a diagonal at the top right, as are paths and small groups of trees in the Embarcadero Marine Park, just below the marina at the upper right. Photos courtesy of Space Imaging, Inc.

THE NEED FOR PHOTO INTERPRETERS

Two incidents underscore the difficulty of interpreting even not-so-subtle images. A convincing sign of planned Soviet missile deployments in Cuba in 1962 was an image of a peculiar road pattern called "the Star of David" because of its resemblance to that religious symbol. To the untrained eye it looked like an odd road interchange, but trained U.S. photo interpreters recognized it as a pattern they had seen before—in Soviet missile fields. Without explaining the image, and perhaps without showing photos of Soviet missile fields, interpreters could have faced ridicule from policy makers.

In the late 1970s and early 1980s, when Cuba was sending expeditionary forces to various parts of the Third World, newly constructed baseball fields indicated their arrival. To understand the significance of these fields, policy makers need to know that Cuban troops play baseball for recreation. Interpreters would have to supply supporting analysis, perhaps a note explaining how serious Cubans take baseball, to avoid being dismissed out of hand. New fields, in this case, could have meant large troop concentrations.

expanded the overall collection capability of the United States and allowed it to reserve more sophisticated imagery capabilities for those areas where they were most needed, while *IKONOS* took up other collection tasks. As noted earlier, use of this commercial imagery makes it easier for the United States to share imagery with other nations or the public without revealing classified capabilities. At the same time, foreign governments that may be hostile to the United States or may see the Afghanistan campaign as a means of gauging U.S. military capabilities were denied access to imagery. The purchase also denied the use of this commercial imagery to news media, which might be eager to use it as a means of reporting on and assessing the conduct and success of the war.

An ancillary effect of the purchase of commercial imagery was to circumvent the shutter control issue. The United States can impose shutter control over commercial satellites operated by U.S. companies for reasons of national security. Concerns arose that civil liberties groups or the news media would mount a legal challenge to an assertion of shutter control, the outcome of which was uncertain. By simply purchasing the imagery, NIMA avoided the entire issue. (The French Ministry of Defense banned the sale of *SPOT* images of the Afghan war zone. The French commercial satellite *SPOT* has a 10-meter resolution.)

Increased use of commercial imagery to support intelligence has become official U.S. intelligence policy. In June 2002, DCI Tenet ordered that commercial imagery would be "the primary source of data for government mapping," with government satellites to be used for this purpose only in "exceptional circumstances." Tenet had two goals: to reserve higher resolution satellites for collection tasks more demanding than map making and to provide a base for a continuing U.S. commercial satellite capability. This policy was expanded in April 2003, when President George W. Bush signed a directive stating that the United States would rely on commercial imagery "to the maximum practical extent" for a wider range of requirements: "military, intelligence, foreign policy, homeland security and civil uses." Again, U.S. government systems are to be reserved for the more demanding collection tasks.

In addition to shutter control, the U.S. government reserves the right to limit collection and dissemination of commercial imagery. (The secretary of commerce regulates and licenses the U.S. commercial imagery industry. The secretaries of state and defense determine policy with regard to protecting national security and foreign policy concerns.) The new policy also allows the use of foreign commercial imagery. NGA's current contracts with commercial imagery firms call for 0.5 meter resolution (1.6 ft.) by 2006. One U.S. company has applied to the Department of Commerce for a 0.25 meter (less than 10 in.) resolution.

A second major imagery development has centered on UAVs. The use of pilotless drones for imagery is not new, but their role and capability have expanded greatly. UAVs offer two clear advantages over satellites and manned aircraft. First, unlike satellites, they can fly closer to areas of interest and loiter over them instead of making a high-altitude orbital pass. Second, unlike manned aircraft, UAVs do not put lives at risk, particularly from surface-to-air missiles (SAMs). Not only are UAVs unmanned, but operators also can be safely located great distances (even thousands of miles) from the area of operation, linked to the UAV by satellite. A third advantage is that the UAVs produce real-time images—they carry high-definition television and infrared cameras—that is, video images are immediately available for use instead of having to be processed and exploited first. This capability helps obviate the "snapshot" problem. In 2006, the Senate Intelligence Committee stated that it wanted NGA to be able to provide video and images to troops via laptop computers, thus increasing tactical imagery support.

The United States currently relies on two UAVs, the Predator and the Global Hawk. Predator operates at up to twenty-five thousand feet, flying at the relatively slow speeds of 84 to 140 miles per hour. It can be based as far as 450 miles from a target and operate over the target for sixteen to twenty-four hours. Predator provides real-time imagery and has been mated with air-to-ground missiles, allowing immediate attacks on identified targets instead of having to relay the information to nearby air or ground units. In the war on terrorism, Predators have been armed with Hellfire missiles, which are guided to the target by a laser. Thus, once a target has been located and identified, no time is lost in calling in an air strike. The Predator was used in this manner against al Qaeda terrorists in Yemen and a senior al Qaeda leader in Pakistan. Global Hawk operates at up to sixty-five thousand feet at a speed of up to four hundred miles per hour. It can be based three thousand miles from the target and can operate over the target for twenty-four hours. Global Hawk is designed to conduct both broad area and continuous spot coverage.

In 2005, Secretary of Defense Donald H. Rumsfeld (2001–2006) talked about building fifteen Predator squadrons (twelve UAVs per squadron) over the next five years, emphasizing both the intelligence collection and the hunter killer missions in which the UAVs carry missiles as well. The Air Force is also looking at the possibility of flying very large drones (perhaps 200 ft. across and 90,000 lbs.) in which the sensors would be embedded in the wings. Planners would like to see these drones stay aloft for up to two days at a time. According to *Scientific American,* DOD is also looking at a UAV that would be launched over the target area via ballistic missile, allowing surveillance of any suspicious location within one hour (assuming the UAV and missile were already mated and poised on a launch pad). Another UAV project seeks to develop a UAV that can remain aloft for up to five years, relying on solar energy or some other easily stored power source. As of September 2007, the record for keeping a UAV aloft is fifty-four hours during the test flight of a British UAV.

A growing number of much smaller UAVs (some weighing as little as two kg. or 4.5 lbs.) can be carried and launched by individuals. These UAVs (sometimes called TUAVs—tactical UAVs) have smaller operating ranges and shorter flight times but are useful for tactical intelligence collection. Some UAV advocates have shown interest in stealth UAVs that could begin collection close to a presumed enemy prior to hostilities without detection. Critics argue that overflights of territory by UAVs would be precluded prior to hostilities (an incursion violating international law) and that therefore stealth is unnecessary.

DOD is also examining the utility of very small satellites, sometimes referred to as microsatellites (approximately twenty inches high and forty-one inches in diameter). *TacSat-1* (tactical satellite) could be launched as demands for collection increased. TacSats would not have the multiyear orbital lives of the more traditional large satellites and would not carry as large a payload of sensors, but they would provide a more flexible collection array and might be useful if satellites were lost to ASATs. Press reports suggest, however, that these satellites still do not have sufficient support within DOD. Tactical satellites also run counter to another U.S. government program, fostering the sharing of satellites by military and domestic agencies. Such satellites would need to have a large array of collectors to be of more general use, which again necessitates a larger satellite.

There have also been several press articles about the possibility of creating microdrones. These are typically compared to dragonflies, and can be as small as six inches (15 cm.) in wingspan. Microdrones are powered so their flight can be controlled and can be equipped with tiny cameras. Microdrones are still experimental and no U.S. agency will acknowledge such a program. These platforms would have the advantage of being relatively inexpensive and could access locations that even UAVs could not target.

The third major imagery development related to the war on terrorism has been the use of NGA imagery platforms on potential terrorist targets within the United States. These have included the 2002 Olympics in Utah, the 2004 political conventions, and other public events that would attract large crowds or locations (such as nuclear power plants) that might be targets. Unlike CIA and NSA, NGA is not restricted in its activity within the United States, although as a defense component NGA cannot be used to support law enforcement. In August 2007, however, the Bush administration announced that it would allow greater access to imagery by state and local officials. Officials argue that this is necessary both to improve homeland security (in such areas as seaport and border security) and also to help with disaster planning or relief. They also argue that these uses do not violate the law enforcement restrictions. Still, various groups that are concerned about intrusive government activities have raised questions about this domestic imagery collection, as have some

members of Congress. In October 2007, the Department of Homeland Security announced postponement of the program to address the legal and civil liberties ramifications.

Finally, space-based imagery capabilities have proliferated. Once the exclusive preserve of the United States and the Soviet Union, this field has expanded rapidly. France and Israel have independent imagery satellites. India has a nascent capability; China is rapidly developing one and has announced that it is building a national engineering and research center to design small satellites, hoping to produce six to eight annually. China plans on launching more than one hundred satellites by 2020 for a variety of monitoring tasks within China itself—economic, ecological, and others. Germany has decided to create its own satellite capability. Furthermore, cooperation among current and would-be imagery satellite powers has increased. Israel is reported to have cooperative imagery relationships with India, Taiwan, and Turkey. Brazil and China are cooperating on satellites. Russia, eager for cash, has helped several nations launch satellites, including Israel, Japan, and Iran. Some experts believe that the Iranians seek an independent launch capability, which could be part of their overall missile development program. Perhaps more significant, France is working with several European partners—Belgium, Italy, and Spain—on its next generation of imagery satellites. This independent capability within NATO could prove troublesome, as the United States may have to deal with allies having their own imagery and different interpretations of events. This apparently happened in 1996, when France refused to support a U.S. cruise missile attack on Iraq because the French maintained that their imagery did not show significant Iraqi troop movements into Kurdish areas. France, Germany, and Israel also have indigenous UAV programs. In 2004, Iran admitted supplying eight UAVs to the Hezbollah terrorist group, one of which penetrated Israeli airspace.

Imagery proliferation also has a commercial aspect. A British firm, Surrey Satellite Technology, has pioneered a range of imagery satellites, including nanosatellites and microsatellites weighing as little as 6.5 kilograms, or just over fourteen pounds. These satellites do not approach resolutions of the best national systems, but they are sufficient for many nations' needs. Among the firm's clients are Algeria, Britain, China, Nigeria, and Thailand. These satellites also have the ability to get close to other satellites and image them, which is of concern to the United States because of their potential to be used as ASAT weapons. Several nations, including Australia, Malaysia, and South Korea, as well as some current Surrey customers, are looking at small satellite demonstration projects.

The proliferation of imagery capabilities could be a problem for the United States should it become engaged in hostilities with a state that has access to space-borne imagery satellites. Therefore, DOD has begun considering countermeasures. One such system, Counter Surveillance Reconnaissance System (CSRS, pronounced "scissors"), would have blinded or dazzled imagery satellites with directed energy. However, Congress refused to fund the program.

SIGNALS INTELLIGENCE. SIGINT is a twentieth-century phenomenon. British intelligence pioneered the field during World War I, successfully intercepting German communications by tapping underwater cables. The most famous product of this work was the Zimmermann Telegram, a 1917 German offer to Mexico of an anti-U.S. alliance, which Britain made available to the United States without revealing how it was obtained. With the advent of radio communications, cable taps were augmented by the ability to pluck signals from the air. The United States also developed a successful signals intercept capability that survived World War I. Prior to World War II, the United States broke Japan's Purple code; Britain, via its ULTRA decrypting efforts, read German codes.

Today, signals intelligence can be gathered by Earth-based collectors—ships, planes, ground sites—or satellites. NSA is responsible for both carrying out U.S. signals intelligence activities and protecting the United States against hostile SIGINT. UAVs, which have been primarily GEOINT platforms, are being used for SIGINT as well. Global Hawk will be configured to carry electronic intelligence (ELINT) and communications intelligence (COMINT) payloads. This enhances the utility of the UAV, as it allows collection synergy between GEOINT and SIGINT on a single platform that can be targeted or retargeted during flight. Greatly increased cooperation between SIGINT and GEOINT has been a recent development. NSA and NGA created a Geocell, which is jointly manned unit that allows quick handoffs between the two INTs, which can be especially important when tracking fast-moving targets, such as suspected terrorist activities.

As with GEOINT, the United States seeks ways to deny enemies their own SIGINT capabilities. Although the CSRS against imagery was not funded, DOD has declared the Counter Communications System operational. The system temporarily jams communications satellites with radio frequencies.

SIGINT consists of several different types of intercepts. The term is often used to refer to the interception of communications between two parties, or COMINT. SIGINT can also refer to the pickup of data relayed by weapons during tests, which is sometimes called telemetry intelligence (TELINT). Finally, SIGINT can refer to the pickup of electronic emissions from modern weapons and tracking systems (military and civil), which are useful means of gauging their capabilities, such as range and frequencies on which systems operate. This is sometimes referred to as ELINT, but is more customarily referred to as FISINT (foreign instrumentation signals intelligence).

The ability to intercept communications is highly important, because it gives insight into what is being said, planned, and considered. It comes as close as one can, from a distance, to reading the other side's mind, a goal that cannot be achieved by imagery. Reading the messages and analyzing what they mean is called **content analysis.** Tracking communications also gives a good **indication and warning.** As with imagery, COMINT relies to some degree on the regular behavior of those being watched, especially among military units. Messages may be sent at regular hours or regular intervals, using known frequencies. Changes in those patterns—either increases or decreases—may be indicative of a larger change in activity. Monitoring changes in communications is known as **traffic analysis,** which has more to do with the volume and pattern of communications than it does with the content. *(See box, "SIGINT Versus IMINT.")* One other important aspect of COMINT is that it provides both content (what is being said) and what might be called texture, meaning the

SIGINT VERSUS IMINT

An NSA director once made a distinction between IMINT—now called GEOINT—and SIGINT: "IMINT tells you what has happened; SIGINT tells you what will happen."

While an exaggeration—and said tongue in cheek—the statement captures an important difference between the two collection disciplines.

tone, the choice of words, the accent (such as when distinguishing one type of French- or Spanish- or Arabic-speaker). Texture is like listening to the tone or watching the facial expression of a speaker. This can tell you as much—or sometimes more—as the words.

COMINT has some weaknesses. First and foremost, it depends on the presence of communications that can be intercepted. If the target goes silent or opts to communicate via secure landlines instead of through the air, then the ability to undertake COMINT ceases to exist. Perhaps the landlines can be tapped, but doing so is a more difficult task than remote interception from a ground site or satellite. The target also can begin to **encrypt**—or code—its communications. Within the offensive-defensive struggle over SIGINT is a second struggle, that between encoders and codebreakers, or **cryptographers.** Crypies, as they are known, like to boast that any code that can be constructed can also be solved. But the present-day is far removed from the Elizabethan age of relatively simple ciphers. Computers greatly increase the ability to construct complex, onetime-use codes. Meanwhile, computers also make it more possible to attack these codes. Finally, the target can use false transmissions as a means of creating less compromising patterns or of subsuming important communications amid a flood of meaningless ones—in effect, increasing the ratio of noise to signals.

Another issue is the vast quantity of communications now available: telephones of all sorts, faxes, e-mails, and so on. In 2002, for example, there were some 180 billion minutes of international phone conversations, from some 2.8 billion cellular phones and 1.2 billion fixed phones. Instant messaging, a relatively new medium, generates 530 billion messages daily. As communications switch to fiber optic cable, the available volume will increase. Also, more phone calls are going over the Internet using the Voice-over-Internet-Protocol (VoIP) technology.

Even a focused collection plan collects more COMINT than can be processed and exploited. One means of coping with this is the **key-word search,** in which the collected data are fed into computers that look out for specific words or phrases. The words are used as indicators of the likely value of an intercept. The system is not perfect, but it provides a necessary filter to deal with the flood of collected intelligence. TELINT and ELINT offer valuable information on weapons capabilities that would otherwise be unknown or would require far more risky human intelligence operations to obtain. However, as the United States learned from its efforts to monitor Soviet arms, the weapons tester can employ many techniques to maintain secrecy. Like communications, test data can be encrypted. It can also be encapsulated—that is, recorded within the weapon being tested and released in a self-contained capsule that will be recovered—so that the data are never transmitted as a signal that would be susceptible to interception. If the data are transmitted, they can be sent in a single burst instead of throughout the test, greatly increasing the difficulty of intercepting and reading the data. Or the data can be transmitted via a spread spectrum, that is, using a series of frequencies through which the data move at irregular intervals. The testing nation's receivers can be programmed to match the frequency changes, but such action greatly increases the difficulty of intercepting the full data stream.

One issue that arises in SIGINT, especially in COMINT, is **risk versus take.** This refers to the need to consider the value of the intelligence that is going to be collected (the take) against the risk of discovery—either in political terms or in the collection technology that may then be revealed to another nation.

The war against terrorism has underscored a growing concern for SIGINT. As with the other collection disciplines, SIGINT was developed to collect intelligence on the Soviet Union and other nations. Terrorist cells offer much smaller signatures, which may not be susceptible to interception by remote SIGINT sensors. Therefore, a growing view is that future SIGINT will have to rely on sensors that have been physically placed close to the target by humans. In effect, HUMINT will become the enabler for SIGINT. Signs also are evident that terrorist groups have increasing knowledge about U.S. SIGINT capabilities and therefore take steps to evade SIGINT detection by such means as using cell phones only once or avoiding cell phones and faxes.

Another SIGINT weakness is found within COMINT—foreign language capabilities. During the cold war, the United States emphasized the need for Russian speakers through a series of government-sponsored educational programs. Today, different languages are at issue: Arabic (which has many spoken varieties), Farsi, Pushto, Dari, Hindi, Urdu, and other languages common to the Middle East and South Asia. None of these languages has much academic support in the United States, and they all have the added difficulty of not being written in the Roman alphabet (which is also true of Russian, Chinese, and some six thousand other languages). It takes about three years (full time) to train someone to the desired capability in a non–Roman language. The United States suffers in its language capabilities because of the decline in language requirements in colleges and universities. According to the Modern Language Association, only 8 percent of schools have language requirements, down from 87 percent in the 1950s through the early 1970s. The United States, being an immigrant nation, has among its citizens speakers of most languages. But they need to be recruited, cleared, and trained. Clearing such candidates is a major motivation in DNI McConnell's efforts to improve the security clearance process. In some cases, the native language skills of these people are very good but their ability to translate into English, which

is the required outcome, is poor. For the foreseeable future, language skills will be a major problem for COMINT and for all intelligence activities.

A more fundamental issue for SIGINT collection in U.S. intelligence has been the capability of NSA to keep pace with the technological changes. It is important to understand that NSA has two roles: offense and defense. NSA intercepts foreign communications but also acts to prevent the interception of U.S. communications. These two roles are very closely allied—in effect, opposite sides of the same coin.

The offense role is made more difficult by the ongoing explosion in the amount of communications worldwide. According to Lucent Technologies, in 2006 there were more than 9.3 trillion e-mails; more than 300 billion voicemail messages; more 18 million new wireless users joining the 1.3 billion already using wireless; more than 123 billion Internet logins; and more than 32 million new phone lines. Again, NSA does not have to track all of these communications, but it does have to find the intercepts it needs inside this vast communications haystack.

Likewise, the defensive role is made more difficult by the increasing number of hacking attempts against government computers. Several new procurement programs designed to upgrade NSA infrastructure ran into cost overruns and failed to produce the needed improvements. There have even been concerns that NSA's obviously high demands for electrical power will soon outstrip available supplies in its home state of Maryland.

The defense role has received increased attention as the number of attacks on U.S. government computers has sharply increased. Defense not only seeks to protect U.S. codes and communications but also the vast array of computers on which the nation relies. In January 2008, President Bush signed a directive authorizing the intelligence community—especially NSA—to monitor the networks of all federal computers as a means of detecting and defending against external attacks. According to press reports, NSA, CIA and the Federal Bureau of Investigation (FBI) will investigate intrusions by monitoring and reporting on Internet activity. This directive raised concerns about intelligence agencies looking into domestic activities but also was criticized by those concerned about cyber security, because the directive does not include the private sector, where some believe the real danger lies—banks, utilities, and other parts of the critical infrastructure.

An important aspect of SIGINT operations for the United States in combating terrorism is the legal issues involved. Under pre-2001 rules, if the SIGINT target was within the United States, the operation became the responsibility of the FBI, not NSA. To undertake wiretaps in the United States, the FBI must get a court order. Foreign intelligence wiretaps (as opposed to criminal case wiretaps) come under the jurisdiction of the Foreign Intelligence Surveillance Act (FISA) Court, created by the FISA in 1978. This was not seen as a major legal barrier, as the FISA court has reportedly approved 13,164 requests and denied four since its inception. In addition, according to data provided by the court to the Congress, the court approved more than 99.9 percent of all requests for wiretaps between 2000 and 2006.

The changing nature of communications and the campaign against terrorists have also led to requests by U.S. intelligence to change the rules under which they collect SIGINT within the United States. Since 1978, these activities had been conducted under FISA. Although FISA allowed for warrantless wiretaps under certain conditions (a one-year limit, conducted on foreign powers only, authorized by the president via the attorney general), press stories in December 2005 revealed a more extensive use of warrantless wiretaps since 2002. These revelations set off a major political controversy concerning the legal basis of the program as well as efforts to revise the law to adjust to changing circumstances. The details of this controversy are beyond the scope of this book, except to note that not only was there disagreement between the Bush administration and some in Congress over the new wiretap program but also among members of the Bush administration as well.

The new warrantless taps President Bush allowed after the September 11, 2001, attacks were placed on calls between people in the United States and terrorist suspects abroad. The Bush administration argued that the new program was necessary as the taps had to be placed quickly and this did not allow time to go to the FISA court. Judge Royce C. Lamberth, who headed the court from 1995–2002, refuted this argument, saying that court procedures had been streamlined in 2001 to make the court more responsive. In August 2007, DNI McConnell revealed that legal changes were necessary because a judge on the FISA court had ruled that court-sanctioned warrants were required on any communications traveling through the United States, even if the two parties involved in the exchange were both overseas. This was seen as a major setback for surveillance, as many Internet communications will pass through the United States. According to press reports, intelligence officials said this ruling had resulted in a 25 percent drop in intercepts. McConnell also revealed that one hundred or fewer individuals in the United States were under surveillance. He also acknowledged that some telecommunications companies had assisted the warrantless surveillance program.

After an intense and partisan debate that lasted almost a year, Congress passed a new law in July 2008 that was largely seen as a victory for the Bush administration. The law allows emergency wiretaps on American targets for one week without a warrant to preclude losing important intelligence and if there is strong reason to believe that the target is linked to terrorism. There is a similar one-week provision for foreign targets. Broad warrants, versus specific ones, will be allowed against foreign communications. The law also grants legal immunity to telecommunications firms that cooperated with the earlier warrantless program, which had been a major issue. The new law also makes clear that changes can only be made in the wiretap program within the law and not solely on order of the president. Various oversight provisions by the FISA court and by inspectors general are laid out as well.

A controversy involving U.S. and British SIGINT operations arose in 2004. A Government Communications Headquarters employee alleged that NSA had conducted SIGINT at the UN, against Security Council members, during the debates prior to the war against

Iraq. Both governments refused to confirm the allegations. The UN, by treaty, is deemed to be inviolate from such activity. At the same time, all nations know that the UN is an excellent intelligence collection target as virtually all nations of the world have missions and representatives there. (See chap. 13 for a fuller discussion.)

MEASUREMENT AND SIGNATURES INTELLIGENCE. FISINT and ELINT are both major contributors to a little-understood branch of collection known as MASINT. MASINT refers to weapons capabilities and industrial activities. MSI and HSI also contribute to MASINT.

An arcane debate rages between those who see MASINT as a separate collection discipline and those who see it as simply a product, or even a by-product, of SIGINT and other collection capabilities. For our purposes, it is sufficient to understand that MASINT exists and that, in a world increasingly concerned about such issues as proliferation of weapons of mass destruction, it is of growing importance. For example, MASINT can help identify the types of gases or waste leaving a factory, which can be important in chemical weapons identification. It can also help identify other specific characteristics (composition, material content) of weapons systems.

MASINT practitioners think of their INT as having six disciplines.

1. Electro-optical: the properties of emitted or reflected energy in the infrared to ultraviolet part of the spectrum, including lasers and various types of light—infrared, polarized, spectral, ultraviolet, and visible
2. Geophysical: the disturbance and anomalies of various physical fields at, or near, the surface of Earth, such as acoustic, gravity, magnetic, and seismic
3. Materials: the composition and identification of gases, liquids, or solids, including chemical-, biological-, and nuclear-related material samples
4. Nuclear radiation: the qualities of gamma rays, neutrons, and x-rays
5. Radar: the properties of radio waves reflected from a target or objects, including various types of radars such as line-of-sight and over-the-horizon and synthetic apertures
6. Radio frequency: the electromagnetic signals generated by an object, either narrow- or wide-band

MASINT can be used against a wide array of intelligence issues, including WMD development and proliferation, arms control, environmental issues, narcotics, weapons developments, space activities, and denial and deception practices.

MASINT has suffered as a collection discipline because of its relative novelty and its dependence on the other technical INTs for its products. Often analysts or policy makers look at a MASINT product without knowing it. MASINT is a potentially important INT still struggling for recognition. It is also more arcane and requires analysts with more technical training to be able to use it fully. At present, policy makers are less familiar—and probably less comfortable—with it than they are with GEOINT or SIGINT. Responsibility for

MASINT is shared by the Defense Intelligence Agency (DIA) and NGA; it is not a separate agency. Some of its advocates believe that MASINT will never make a full contribution until it has more bureaucratic clout. Others, even some sympathetic to MASINT, do not believe this INT needs the panoply of a full agency.

HUMAN INTELLIGENCE. HUMINT is espionage—spying—and is sometimes referred to as the world's second-oldest profession. Indeed, it is as old as the Bible. First Moses and then Joshua sent spies into Canaan before leading the Jewish people across the Jordan River. Spying is what most people think about when they hear the word "intelligence," whether they conjure up famous spies from history such as Nathan Hale or Mata Hari (both failures) or fictional spies such as James Bond. In the United States, HUMINT is largely the responsibility of the CIA, through the National Clandestine Service (NCS), formerly known as the Directorate of Operations (DO). The DIA also has a HUMINT capability with the Defense Humint Service, which it has sought to expand since the war in Afghanistan. The FBI and the Drug Enforcement Administration (DEA) also have officers who operate overseas. This multitude of collectors was what led DCI Porter J. Goss to create the NCS. The NCS has three branches: CIA HUMINT; Community HUMINT; and Technology. The Community HUMINT office serves to coordinate among the various agencies conducting HUMINT, a necessary task to avoid duplication of effort or operations that run at cross purposes. The director of the CIA (DCIA) is the HUMINT program manager.

HUMINT largely involves sending clandestine service officers to foreign countries, where they attempt to recruit foreign nationals to spy. The process of recruiting spies has several steps and a unique vocabulary. The process of managing spies is sometimes referred to as the **agent acquisition cycle.** The cycle has five steps.

1. Targeting or spotting: identifying individuals who have access to the information that the United States may desire.
2. Assessing: gaining their confidence and assessing their weaknesses and susceptibility to be recruited; done via the **asset validation system.**
3. Recruiting: making a **pitch** to them, suggesting a relationship; a **source** may accept a pitch for a variety of reasons: money, disaffection with their own government or thrills. U.S. clandestine service officers state very firmly that blackmail is not used, at least by them, to recruit spies.
4. Handling: managing of the asset.
5. Termination: ending the relationship for any of several reasons—unreliability, a loss of access to needed intelligence, a change in intelligence requirements, and so on.

Another HUMINT term of art is the **developmental,** a potential source who is being brought along—largely through repeated contacts and conversations to assess his or her value (validation) and susceptibilities—to the point where the developmental can be pitched. If and when the pitch has been accepted, the officer must meet with this new source

regularly to receive information, holding meetings in a manner and in places that reduce the risk of being caught and then transmitting the information back home. The source may rely on sources of his or her own, known as **sub-sources,** to provide intelligence that the original source then conveys to the agent.

Diplomatic reporting is a type of HUMINT, although it tends to receive less credibility in some circles because of its overt nature. After all, the foreign government official knows, when speaking to a diplomat, that his or her remarks are going to be cabled to that diplomat's capital. An espionage source is likely to be thinking the same thing. Nonetheless, some people prefer more traditional HUMINT, even if the source's reliability remains uncertain, rather than diplomatic reporting.

HUMINT requires time to be developed. Clandestine service officers need to learn a variety of skills (foreign languages; conducting, detecting, or evading surveillance; recruiting skills and other aspects of HUMINT tradecraft; the ability to handle various types of communications equipment; weapons training; and so on). Like all other professions, it takes time to become adept. In the case of HUMINT officers, it takes up to seven years, according to some accounts.

In addition to gaining the skills required for this activity, officers have to maintain their cover stories—the overt lives that give them a plausible reason for being in that foreign nation. There are two types of cover: official and nonofficial. Officers with **official cover** hold another government job, usually posted at the embassy. Official cover makes it easier for the agent to maintain contact with his or her superiors but raises the risk of being suspected as an agent. **Nonofficial cover** (NOC, pronounced "knock") avoids any overt connection between the officer and his or her government but can make it more difficult to keep in contact. NOCs need a full-time job that explains their presence; they cannot make contact with superiors or colleagues overtly. (This led to a bureaucratic problem for the CIA in that NOCs had to at least appear to be paid at a level commensurate with their cover job, which was sometimes higher than their government salary. This then raised the issue of being liable for taxes higher than their actual salary. Congress authorized the CIA to pay NOCs "in a manner consistent with their cover.")

For the CIA, at least, some limits exist on the jobs that NOCs can hold. Clergy and Peace Corps volunteers are off-limits. Journalism is an ideal cover for a NOC, as journalists have a plausible reason for being in a foreign country, for seeking out officials, and for asking questions. However, professional journalists have long protested any such use of cover, arguing that if one spy posing as a journalist were to be unmasked, then all journalists would be suspect and perhaps in danger. Proponents counter that journalism is a profession like any other and should be available for use. All told, the use of NOCs is more complex than is official cover for spies.

Some HUMINT sources volunteer. They are called **walk-ins.** Spies Oleg Penkovsky of the Soviet Union, Aldrich Ames of the CIA, and Robert Hanssen of the FBI were all walk-ins. Walk-ins raise a host of other issues: Why have they volunteered? Do they really have access to valuable intelligence? Are they real volunteers or a means of entrapment—called **dangles**? Dangles can be used for a number of purposes, including identifying hostile intelligence personnel or gaining insights into the intelligence requirements or methods of a hostile service. According to press accounts reporting on the investigation led by former FBI director and DCI (1987–1991) William H. Webster, the Soviet Union suspected that Hanssen was a dangle and protested to the United States. The United States denied the charge but did not follow up.

In addition to recruiting foreign nationals, HUMINT officers may undertake more direct spying, such as stealing documents or planting sensors. Some of their information may come through direct observation of activity. Thus, HUMINT can involve more INTs than just espionage.

An important adjunct to one's own country's HUMINT capabilities are those of allied or friendly services. Known as **foreign liaison** relationships, these offer several important advantages. First, the friendly service has greater familiarity with its own region. Second, its government may maintain a different pattern of relations with other states, more friendly in some cases or even having diplomatic relations where one's own government does not. These HUMINT-to-HUMINT relationships are somewhat formal in nature and tend to be symbiotic. They also entail risks, as one can never be entirely sure of the liaison partner's security procedures. Thus, there are different degrees of liaison, depending on past experience, shared needs, the sense of security engendered, the depth and value of the intelligence being shared, and so forth. Furthermore, some liaison relationships may be with intelligence services that do not have the same standards in terms of operational limits, acceptable activities, and other criteria. A choice therefore has to be made between the value of the information being sought or exchanged and the larger question of the propriety of a relationship with this service. Nevertheless, liaison is an important means of increasing the breadth and depth of available HUMINT.

Foreign intelligence liaison is carried out on an agency-by-agency basis instead of by the intelligence community as a whole. The CIA, DIA, NGA, and NSA, for example, create and conduct their own liaison relationships, which does raise questions about the possible need for better coordination to avoid duplication. Thus, the stovepipes problem carries over into foreign liaison. This may prove to be a problem for the DNI who is charged with overseeing the coordination of these relationships.

In the war against terrorism, several nations have apparently offered intelligence support to the United States, including some whose services may be considered occasionally hostile. These types of liaison relationships call for extra caution regarding intelligence sharing, and questions may arise about the depth and detail of the intelligence received. However, exchanging useful intelligence is a good way for nations to build confidence in one another. For example, according to press accounts, Russian officers placed nuclear detection equipment in North Korea at the request of the United States to help track possible nuclear developments.

Espionage provides a small part of the intelligence that is collected. GEOINT and SIGINT produce a greater volume of intelligence. But HUMINT, like SIGINT, has the major advantage of affording access to what is being said, planned, and thought. Moreover, clandestine human access to another government may offer opportunities to influence that government by feeding it false or deceptive information. For intelligence targets in which the technical infrastructure may be irrelevant as a fruitful target—such as terrorism, narcotics, or international crime, where the signature of activities is small—HUMINT may be the only available source.

HUMINT also has disadvantages. First, it cannot be done remotely, as is the case with various types of technical collection. It requires proximity and access and therefore must contend with the counterintelligence capabilities of the other side. It is also far riskier, as it jeopardizes individuals and, if they are caught, could have political ramifications that are less likely to occur with technical collectors.

HUMINT is far less expensive than the various technical collectors, although it still involves costs for training, special equipment, and the accoutrements clandestine officers need to build successful cover stories.

Like all the other collection INTs, HUMINT is susceptible to deception. Some critics argue that it is the most susceptible to deception. The bona fides of human sources are always subject to question initially and, in some cases, may never be wholly resolved. Many questions arise and linger. Why is this person offering to pass information—ideology, money, vengeance? The person will claim to have good access to valuable information, but how good is it? Is it consistent, or is this a single event? How good is the information? Is this person a dangle, offered as a means of passing information that the other side wants to have passed—either because it is false or because it will have a specific effect? Is this person a double agent who is collecting information on your intelligence agency's HUMINT techniques and capabilities even as he or she passes information to you?

HUMINT officers must walk a fine line between prudent caution and the possibility that too much caution will lead them to deter or reject a promising source. For example, the United States initially rejected the services of Penkovsky, who then turned to the British, who accepted him. Only later did the United States take on this valuable spy. Deception is particularly difficult to deal with, because people naturally are reluctant to accept that they are being deceived. However, people might slip into a position where they trust no one, which can result in turning away sources who might have been valuable.

HUMINT's unique sources and methods raise another issue. These sources are considered to be extremely fragile, given that good human penetrations take so long to develop and risk the lives of the case officers, their sources, and perhaps even the sources' families. Therefore, the intelligence analysts who receive HUMINT reports may not be told the details of the source or sources. Analysts are not informed, for example, that "this report comes from a first secretary in the Fredonian Foreign Ministry." Instead, the report includes information on the access of the source to the intelligence, the past reliability of the source,

or variations on this concept. Sometimes several sources may be blended together in a single report. Although the masking of HUMINT sources promotes their preservation, it may have the unintended effect of devaluing the reports for analysts, who may not fully appreciate the value of the source and the information. This became an issue in the aftermath of the Iraq WMD experience, when it was recognized that some sources had been of questionable reliability and that analysts were not always given as much information as would have been desirable about the nature of some of the HUMINT reporting. It also denies all-source analysts the ability to make an independent judgment of the HUMINT source when compared with the other sources to which they have access. (HUMINT reports come with captions provided by reports officers as to the nature of the source: a reliable source, an untested source, a source with proven access, a source with unknown access, and so on.)

Also, as DCI Richard Helms (1966–1973) observed, most HUMINT sources are recruited for a specific assignment or requirement, based on their access to the desired intelligence. They cannot be assigned from issue to issue as they are extremely unlikely to have access to other intelligence. Helms also believed that spies who no longer had the desired access should not be held in reserve but should be dropped. He said that a well-run station (the base from which officers operate overseas) "does not cling to spent spies." Thus, even successful HUMINT, although extremely valuable, is narrow in focus.

HUMINT also puts one in contact—and perhaps into relationships—with unsavory individuals such as terrorists and narco-traffickers. If one is going to penetrate such groups or develop other types of relationships with them, some may become recipients of money or other forms of payment. These types of relationships raise moral and ethical issues for some people (see chap. 13). In the aftermath of the September 2001 attacks, special attention was given to the so-called Deutch rules about HUMINT recruitment. In 1995, DCI John M. Deutch (1995–1997) ordered a scrub of all HUMINT assets, with a particular focus on persons who in the past had been involved in serious criminal activity or human rights violations. The scrub was the result of revelations that some past CIA assets in Guatemala had violated human rights, including those of some American residents in that country. New rules were promulgated, requiring headquarters approval of any such recruitments in the future. After the terrorist attacks, the rules were widely criticized, with many people asserting that they had limited the CIA's ability to penetrate terrorist groups. CIA officials maintained that no valuable relationship was ever turned down because of the Deutch rules. Critics countered, however, that the very existence of the rules bred timidity in the DO, as officers would be more cautious about whom they recruited, running the risk of losing useful sources, instead of having these recruitments be scrutinized on the basis of changing standards. By the end of 2001, the Deutch rules were no longer considered an operational factor as field stations were told they could be ignored. In July 2002 they were formally rescinded. Writing in the aftermath of the September 2001 attacks, Deutch defended his rules, arguing that they allowed DO officers to recruit with clear guidelines and focused on acquiring high-quality agents.

In the United States, constant tension exists between HUMINT and the other collection disciplines. The dominance of technical collection periodically gives rise to calls for a greater emphasis on HUMINT. So-called intelligence failures, such as the fall of the shah of Iran in 1979, the unexpected Indian nuclear tests in 1998, and the 2001 terrorist attacks have led to demands for more HUMINT. There is something odd about this recurring call for more HUMINT in that successful HUMINT is not a question of the mass of agents being assigned to a target. Some targets, such as terrorist cells, or the inner sanctum of totalitarian regimes, will always be difficult to penetrate. There is no reason to believe that the twentieth agent who is sent will succeed when the first nineteen have not. It is not possible to swarm agents against a difficult HUMINT target in terms of the agents' availability and, more important, the risk. Such an effort would be more likely to alert the target to possible penetration attempts, further hampering HUMINT.

Again, no right balance can be struck between HUMINT and the other collection disciplines. Such an idea runs counter to the concept of an all-source intelligence process that seeks to apply as many collection disciplines as possible to a given intelligence need. But not every collection INT makes an equal or even similar contribution to every issue. Clearly, having a collection system that is strong and flexible and can be modulated to the intelligence requirement at hand is better than one that swings between apparently opposed fashions of technical and human collection.

As with all other INTs, it is difficult, if not impossible, to put an ultimate value on HUMINT. It is one of the two most democratic INTs (along with OSINT), because any nation or group can conduct HUMINT. Clearly, it would be preferable to have good HUMINT access for key issues. But cases such as Ames and Hanssen raise questions about HUMINT's value. These two spies provided the Soviet Union and post–Soviet Russia with invaluable information, largely about U.S. spy penetrations in that country but also, in the case of Hanssen, about technical collection operations and capabilities. When their activities are added to past espionage revelations—such as Kampiles (IMINT), the Walkers (SIGINT), and Pelton (SIGINT)—the Soviet Union and post–Soviet Russia gained substantial knowledge about U.S. collection capabilities. Yet the Soviet Union lost the cold war and ceased to exist as a state. One could argue, on the one hand, that all of this HUMINT ultimately proved to be of no value, thus raising questions about HUMINT's utility. On the other hand, one could argue that no amount of HUMINT—or any other INT—can save a state that has profound internal problems.

Critics of HUMINT argue that the most important spies (Penkovsky, Ames, Hanssen, and many others) have tended to be walk-ins rather than recruited spies, which raises a serious question about HUMINT capabilities. If one accepts the idea that collection is a synergistic activity, then even the recruitment of lower-level spies adds to one's overall knowledge. Also, even if the most productive spies are walk-ins, some sort of apparatus is needed to handle them, to get out the intelligence they provide, and so on.

One of the major concerns in HUMINT is the possibility that a clandestine officer will be caught and unmasked, with attendant personal risk for the officer and political embarrassment for the state that sent the officer. Even a successful long-term espionage penetration can prove costly. The case of Gunter Guillaume is illustrative. Guillaume was an East German spy who was able to penetrate the West German government, rising to a senior position in the office of Chancellor Willy Brandt. When Guillaume's espionage was uncovered in 1974, Brandt was forced to resign. Many people believed that the political cost of the operation exceeded any gains in intelligence. Brandt's *Ostpolitik*—or favorable policy toward East Germany—was never resumed by his successors, at great cost to East Germany, perhaps even greater than any intelligence that Guillaume produced over the years. Similarly, the fate of Jonathan Pollard (see chap. 15 for more details), who passed classified intelligence to Israel, became a constant irritant in U.S.–Israeli relations, again outweighing the value of the intelligence that Pollard provided.

The state of HUMINT remains a concern in the U.S. intelligence community. HUMINT suffered from budget cuts through the 1990s, as did all aspects of intelligence. Several officials have noted that the FBI had more agents assigned to New York City than did the DO worldwide. President Bush ordered a 50 percent increase in the number of DO (now NCS) officers. As noted, it will be seven years from their entry on duty (EOD) before these officers are considered fully operational. Porter Goss's tenure as DCI and then DCIA saw the departure of many DO veterans, owing to friction with Goss's staff. This seems to have eased under DCIA Michael Hayden but there have been press reports indicating that attrition rates in the NCS remained high, especially in the five- to ten-year cadre.

For the United States, at least, it remains important to view HUMINT as part of a larger collection strategy instead of as the single INT that meets the country's most important intelligence needs. To place that sort of expectation on any one INT is bound to set it up for disappointment at best and perhaps even failure.

OPEN-SOURCE INTELLIGENCE. To some, OSINT may seem like a contradiction in terms. How can information that is openly available be considered intelligence? This question reflects the misconception that intelligence must inevitably be about secrets. Much of it is, but not to the exclusion of openly available information. Even during the height of the cold war, according to one senior intelligence official, at least 20 percent of the intelligence about the Soviet Union came from open sources.

OSINT includes a wide variety of information and sources.

- Media: newspapers, magazines, radio, television, and computer-based information
- Public data: government reports, official data such as budgets and demographics, hearings, legislative debates, press conferences, and speeches
- Professional and academic: conferences, symposia, professional associations, academic papers, and experts

In addition to these open sources, each of the classified INTs has an OSINT component. The most obvious is commercial imagery. One can also conduct a variety of SIGINT–type activities on the Worldwide Web, such as traffic analysis (the number of people who visit a

SOME INTELLIGENCE HUMOR

In addition to GEOINT, SIGINT, HUMINT, OSINT, and MASINT, intelligence officers, in their lighter moments, speak of other INTs (collection disciplines). One of the most famous is PIZZINT—pizza intelligence. This refers to the belief that Soviet officials based in Washington, D.C., would keep watch for large numbers of pizza delivery trucks going late in the evening to the CIA, DOD, the State Department, and the White House as an indication that a crisis was brewing somewhere. The notion was that, after seeing many trucks making deliveries, the officials would hurry back to the Soviet embassy to alert Moscow that something must be going on somewhere in the world.

Some other INTs that intelligence officers talk about are

LAVINT: lavatory intelligence, such as heard in restrooms,

RUMINT: rumor intelligence,

REVINT: revelation intelligence, and

DIVINT: divine intelligence.

Web site) or changes in Web sites. Given that some aspects of MASINT are related to geophysical phenomena, there are open aspects of MASINT. Finally, there is open HUMINT—the use of overt experts for their own knowledge or as sources of elicitation. This list is by no means exhaustive, but it does give a feel for the range of OSINT within the other INTs. *(See box, "Some Intelligence Humor.")*

One of the hallmarks of the post–cold war world is the increased availability of OSINT. The ratio of open source to classified intelligence on Russia has more than reversed from its 20:80 ratio during the cold war. The number of closed societies and **denied areas** has decreased dramatically. Many of the former Warsaw Pact states are now NATO allies. This does not mean that classified collection disciplines are no longer needed, but that the areas in which OSINT is available have expanded.

The major advantage of OSINT is its accessibility, although it still requires collection. OSINT needs less processing and exploitation than the technical INTs or HUMINT, but it still requires some P&E. Given the diversity of OSINT, it may be more difficult to manipulate for the purpose of deception than are other INTs. OSINT is also useful for helping put the secret information into a wider context, which can be extremely valuable. DNI McConnell has referred to OSINT as the starting point for collection, as have others before him—in other words, looking for the needed intelligence in open sources first before tasking classified collection sources, either technical or human. Putting this seemingly obvious plan into practice has proven difficult over the years for a number of reasons, including preferences within the intelligence community and among policy makers for classified sources and the difficulty that the intelligence community's open source activity has had in keeping pace with the explosion of open sources.

The main disadvantage of OSINT is its volume. In many ways, it represents the worst wheat and chaff problem. Some argue that the so-called information revolution has made OSINT more difficult without a corresponding increase in usable intelligence. Computers

have increased the ability to manipulate information; however, the amount of derived intelligence has not increased apace.

The OSINT phenomenon **echo** is the effect of a single media story being picked up and repeated by other media sources until the story takes on a much larger life of its own, appearing more important than it actually is. Echo is difficult to deal with unless one is aware of the original story and can therefore knowingly discount its effect.

Popular misconceptions about OSINT persist, even within the intelligence community. OSINT is not free. Buying print media costs the intelligence community money, as do various other services that are useful—if not essential—in helping analysts manage, sort, and sift large amounts of data more efficiently. Another misconception is that the Internet or, more properly, the Worldwide Web, is the main fount of OSINT. Experienced intelligence practitioners have discovered that the Internet—meaning searches among various sites—yields no more than 3 to 5 percent of the total OSINT take. That is why practitioners spend much time on what is called the "Deep Web," meaning that much larger portion of the Web that has not been indexed by search engines. Some experts estimate that the Deep Web is roughly some 500 times bigger than the easily accessible Web.

Even though OSINT has always been used, it remains undervalued by significant segments of the intelligence community. This attitude derives from the fact that the intelligence community was created to discover secrets. If OSINT could largely meet the United States' national security needs, the intelligence community would look very different. Some intelligence professionals have mistakenly equated the degree of difficulty involved in obtaining information with its ultimate value to analysts and policy makers. Contributing to this pervasive bias is that OSINT has always been handled differently by the intelligence community. All of the other INTs have dedicated collectors, processors, and exploiters. With the exception of the DNI's Open Source Center (formerly the Foreign Broadcast Information Service, FBIS), which monitors foreign media broadcasts, OSINT does not have dedicated collectors, processors, and exploiters. Instead, analysts are largely expected to act as their own OSINT collectors, a concept that other INTs would consider ludicrous. This is unfortunate, because OSINT is the perfect place to start any intelligence collection. By first determining what material is available from open sources, intelligence managers could focus their clandestine collectors on those issues for which such means were needed. Properly used, OSINT could be a good intelligence collection resource manager. The 2004 intelligence law mandates that the DNI must decide how he or she wishes to deal with OSINT, either by creating a dedicated OSINT center or by some other means. The WMD Commission (the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction) recommended that the CIA create an Open Source Directorate. President George W. Bush endorsed this recommendation and left its implementation to the DNI. DNI Negroponte designated FBIS as the Open Source Center and made the CIA his executive agent (i.e., operating office) to run it. Some felt that little had changed other than renaming FBIS, which had been a CIA office. Its designation as a DNI office did not result in added leverage. The situation was further confused by the creation of an

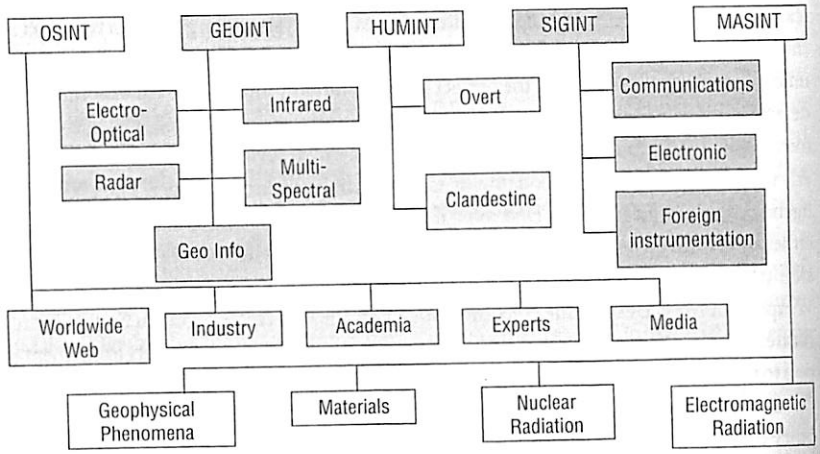
assistant deputy DNI (ADDNI) for open source under the deputy DNI for collection. This ADDNI is responsible for open-source policy but does not control any open-source assets or agencies, including the Open Source Center. The ADDNI/Open Source seeks to create a National Open Source Enterprise that will, among other things, emphasize professional training and certification in the skills required to conduct open-source intelligence, which would be a major step forward.

The 1999 Kosovo air war produced a new OSINT stream. Individuals in Serbia who said they were opposed to the Slobodan Milosevic government sent e-mails to intelligence firms in the United States, giving reports on the relative success of NATO air strikes, the mood in Belgrade, and related matters. Dealing with such reports is problematic as no assured means exists of authenticating them. The most reliable reports would come from known and trusted sources, probably based on past reporting. Establishing an independent capability to accomplish this may not be possible during hostilities. Some sources may prove to be reliable over time. But one has to be on guard for the possibility, if not the likelihood, of at least some level of disinformation from the targeted regime. In the case of Kosovo, at least some of the sources proved to be reliable, thus establishing a new OSINT stream.

CONCLUSION

Each collection discipline is made up of several distinct types of sources (see Figure 5-1) and each offers unique advantages that are well suited to some types of intelligence requirements but brings with it certain disadvantages as well (see Table 5-1). By deploying a broad and varied array of collection techniques, the United States derives two advantages. First,

Figure 5-1 **Intelligence Collection: The Composition of the INTs**



This schematic provides a guide to the types of intelligence within each of the five major INTs.

Table 5-1 **A Comparison of the Collection Disciplines**

INT	Advantages	Disadvantages
GEOINT	Graphic and compelling	Perhaps overly graphic and compelling
	Use seems familiar to policy-makers	Still requires interpretation
	Ready availability of some targets—particularly military exercises	Literally a snapshot of a moment; very static
	Can be done remotely	Subject to problems of weather, spoofing
		Expensive
SIGINT	Offers insights into plans, intentions	Signals may be encrypted or encoded—requiring them to be broken
	Voluminous material	Voluminous material
	Military targets tend to communicate in regular patterns	May encounter communications silence, use of secure lines, spoofing via phony traffic
	Can be done remotely	Expensive
HUMINT	Offers insights into plans, intentions	Riskier in terms of lives, political fallout
	Relatively inexpensive	Requires more time to acquire and validate sources
		Problems of dangles, false feeds, double agents
MASINT	Extremely useful for issues such as proliferation	Expensive
	Can be done remotely	Little understood by most users
		Requires a great deal of processing and exploitation
OSINT	More readily available	Voluminous
	Extremely useful as a place to start all collection	Less likely to offer insights available from clandestine INTs

Note: INT = collection discipline; GEOINT = geospatial (formerly imagery) intelligence; SIGINT = signals intelligence; HUMINT = human intelligence; MASINT = measurement and signatures intelligence; and OSINT = open-source intelligence.

it is able to exploit the advantages of each type of INT, which, ideally, will compensate for the shortcomings of the others. Second, it is able to apply more than one collection INT to an issue, which enhances the likelihood of meeting the collection requirements for that issue. However, the intelligence community cannot provide answers to every question that is asked, nor does it have the capability to meet all possible requirements at any given time. The collection system is simultaneously powerful and limited.

The cost of collection was rarely an issue during the cold war because of the broad political agreement on the need to stay informed about the Soviet threat. In the post–cold war world, prior to the September 2001 attacks, the absence of any overwhelming strategic

threat made the cost of collection systems more difficult to justify. As a result, some people questioned whether a need existed for the level of collection capability that the United States maintained during the cold war. Prior to the terrorist attacks, the United States experienced greatly diminished threats to its national security but faced ongoing concerns that are more diverse and diffuse than was the largely unitary Soviet problem, raising new collection challenges. As horrific as the September 2001 attacks were, terrorism still does not pose the same potentially overwhelming threat to the existence of the United States as did a hostile nuclear-armed Soviet missile force. Ultimately, no yardstick can measure national security problems against a collection array to determine how much collection is enough. For the near future, collection requirements likely will continue to outrun collection capabilities.

KEY TERMS

agent acquisition cycle
all-source intelligence
ASAT (antisatellite)
asset validation system
automatic change extraction
collection disciplines
content analysis
cryptographers
dangles
deception
denial
denied areas
denied targets
developmental
echo
encrypt
espionage
foreign liaison
geosynchronous orbit
indication and warning
key-word search
negation search
noise versus signals
non-official cover
official cover
pitch
resolution
risk versus take
shutter control
source
sources and methods
spies
sub-sources
sun-synchronous orbits
swarm ball
traffic analysis
walk-ins
wheat versus chaff

FURTHER READINGS

For ease of use, these readings are grouped by activity. Although there are numerous books by spies and about spying, few of them have good discussions of the craft of espionage and the role it plays, as opposed to its supposed derring-do aspects.

General Sources on Collection

Best, Richard A., Jr. *Intelligence, Surveillance, and Reconnaissance (ISR) Programs: Issues for Congress.* Washington, D.C.: Congressional Research Service, updated August 24, 2004.
Burrows, William. *Deep Black: Space Espionage and National Security.* New York: Random House, 1986.
Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision.* Stanford: Stanford University Press, 1962.

Espionage

Burgstaller, Eugen F. "Human Collection Requirements in the 1980's." In *Intelligence Requirements for the 1980's: Clandestine Collection.* Ed. Roy F. Godson. Washington, D.C.: National Strategy Information Center, 1982.
Hitz, Frederick P. "The Future of American Espionage." *International Journal of Intelligence and Counterintelligence* 13 (spring 2000): 1–20.
———. *The Great Game: The Myth and Reality of Espionage.* New York: Alfred Knopf, 2004.
Hulnick, Arthur S. "Intelligence Cooperation in the Post–Cold War Era: A New Game Plan?" *International Journal of Intelligence and Counterintelligence* 5 (winter 1991–1992): 455–465.
Phillips, David Atlee. *Careers in Secret Operations: How to Be a Federal Intelligence Officer.* Frederick, Md.: Stone Trail Press, 1984.
Wirtz, James J. "Constraints on Intelligence Collaboration: The Domestic Dimension." *International Journal of Intelligence and Counterintelligence* 6 (spring 1993): 85–89.

Imagery

Baker, John C., Kevin O'Connell, and Ray A. Williamson, eds. *Commercial Observation Satellites: At the Leading Edge of Transparency.* Washington, D.C.: RAND Corporation, 2001.
Best, Richard A., Jr. *Airborne Intelligence, Surveillance, and Reconnaissance (ISR): The U-2 Aircraft and Global Hawk UAV Programs.* Washington, D.C.: Library of Congress, Congressional Research Service, 2000.
Brugioni, Dino A. "The Art and Science of Photo Reconnaissance." *Scientific American* (March 1996): 78–85.
———. *Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis.* Ed. Robert F. McCort. New York: Random House, 1990.
———. *From Balloons to Blackbirds: Reconnaissance, Surveillance, and Imagery Intelligence—How It Evolved.* McLean, Va.: Association of Former Intelligence Officers, 1993.
Central Intelligence Agency. *CORONA: America's First Satellite Program.* Ed. Kevin C. Ruffner. Washington, D.C.: CIA, 1995.
Day, Dwayne A., and others, eds. *Eye in the Sky: The Story of the CORONA Spy Satellites.* Washington, D.C.: Smithsonian Institution Press, 1998.
Lindgren, David T. *Imagery Analysis in the Cold War.* Annapolis, Md.: U.S. Naval Institute Press, 2000.
Peebles, Christopher. *The CORONA Project: America's First Spy Satellite.* Annapolis, Md.: U.S. Naval Institute Press, 1997.
Richelson, Jeffrey T. *America's Secret Eyes in Space: The U.S. Keyhole Spy Satellite Program.* New York: Harper and Row, 1990.
———. "High Flyin' Spies." *Bulletin of the Atomic Scientists* 52 (September–October 1996): 48–54.
Shulman, Seth. "Code Name CORONA." *Technology Review* 99 (October 1996): 23–25, 28–32.
SPOT Image Corporation. *Satellite Imagery: An Objective Guide.* Reston, Va.: SPOT Image Corporation, 1998.
Taubman, Philip. *Secret Empire: Eisenhower, the CIA, and the Hidden Story of America's Space Espionage.* New York: Simon and Schuster, 2003.

Open-Source Intelligence

Best, Richard A., Jr., and Alfred Cumming. "Open Source Intelligence (OSINT): Issues for Congress." Report RL34270. Washington, D.C.: Library of Congress, Congressional Research Service, December 5, 2007.