MARK M. LOWENTHAL

which the intelligence community was created. (It is worth noting that the OSS had an overt branch—Research and Analysis—but it apparently had little legacy in the postwar intelligence community.)

THE COLLECTION DISCIPLINES: 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 is to bring as many collection disciplines as possible to bear on the major issues. The use of multiple disciplines should allow the collectors to gain advantages from mutual reinforcement and from individual capabilities that can make up for shortcomings in the others.

IMAGERY. IMINT is 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. In World Wars I and II both sides used airplanes to obtain photos. Airplanes are still employed, but several nations now employ imagery satellites. In the United States the National Reconnaissance Office (NRO) develops these satellites. The National Imagery and Mapping Agency (NIMA) is responsible for processing and exploiting imagery. Some imagery also comes via the Defense Department's airborne systems, such as unmanned aerial vehicles (UAVs), or drones.

The term *imagery* is somewhat misleading in that it makes most people think of 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 recovered. Modern satellites transmit their images as signals, or data streams, that are received and reconstructed as images.

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). Imagery can also be produced by radar, which has the ability to "see" through cloud cover. Some systems, referred to as multispectral or hyperspectral imagery (MSI and HSI), 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 measurement and signals intelligence (MASINT).

How Much Resolution Is Enough?

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 will allow fairly detailed analysis of man-made objects or subtle changes to terrain. Ten-meter resolution will lose some detail but still will allow the identification of buildings by type or allow surveillance of large installations and associated activity. Twenty- to thirty-meter resolution will cover a much larger area but still will allow 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.

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—one meter, ten meters, and so on. 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. *(See box, "How Much Resolution Is Enough?" this page.)*

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. Indeed, 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 by the simple act of using purposely mis-sized crates to mask the nature of the shipments.)

Imagery offers a number of advantages over other collection means. First, it is sometimes graphic and compelling. When put before policy makers, an easily interpreted image often is worth a thousand words. Second, imagery is easily understood much of the time by policy makers. Even though few, if any, policy makers are trained imagery analysts, all of them are quite accustomed to seeing and interpreting images. From family photos, to newspapers and magazines, to news broadcasts, we all spend an unnoticed part of our day not only looking at images but also interpreting them. Imagery is also easy to use with policy makers in that

The Need for Photo Interpreters—Two Cases in Point

Two incidents underscore the difficulty of interpreting even not-so-subtle images.

One of the signs of planned Soviet missile deployments in Cuba in 1962 was an image of a peculiar road pattern called "the Star of David" for its resemblance to that symbol. To the untrained eye it would look like an odd road interchange, but trained U.S. photo interpreters recognized it as a pattern they had seen before—in Soviet missile fields. But, to run into a senior policy maker's office exulting about a Star of David road pattern without explaining it, and perhaps bringing along samples from imagery of the Soviet Union, might lead to ridicule. Interpreters also found soccer fields—a sign of non-Cuban activity.

In the late 1970s and early 1980s, when Cuba was sending expeditionary forces to various parts of the Third World, one of the signatures of their arrival was newly constructed baseball fields. Cuban troops play baseball for recreation. Again, to inform an official that the Cubans must be in Angola or Ethiopia because we have seen baseball fields is almost ludicrous. Some supporting analysis is required, perhaps including a note that only the United States, Cuba, Mexico, Canada, Japan, and Nicaragua take baseball this seriously, and we can eliminate all of the others as unlikely to have large troop concentrations in these regions.

little or no interpretation is necessary as to how it was acquired. Although the process by which images are taken from space, transmitted to earth, and processed is more complex than using a 35-mm camera, policy customers have enough sense of the process to take it for granted.

Another advantage of imagery is that many of the targets make themselves available. Most nations' militaries exercise on regular cycles and at predictable locations, making them highly susceptible to IMINT. Finally, an image of a certain site will often provide information not just about one activity, but about some ancillary ones as well.

Imagery suffers a number of disadvantages as well. The very graphic quality that is an advantage is also 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 may be contradictory. Also, the intelligence on an image may not be self-evident; it may require interpretation by trained photo interpreters who can "see" things on the image that the untrained person cannot. At times, the policy makers must take on faith

that the skilled analysts are correct. (*See box, "The Need for Photo Interpreters—Two Cases," p. 63.*)

Another disadvantage of imagery is that it is, quite literally, 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, telling you something about where and when it was taken but nothing about what happened before or after the image was taken. Analysts can perform a "negation search," looking at past imagery to determine when an activity commenced. The site can be revisited to watch for further activity. But a single image will not tell you all of this.

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

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 German offer to Mexico of an anti-U.S. alliance that 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 ULTRA, read German codes.

Today, signals intelligence can be gathered by earth-based collectors—ships; planes; or ground sites such as the large Russian facility still functioning in Cuba—or by satellites. Again, U.S. satellites are built by the NRO. The National Security Agency (NSA) is responsible for both carrying out U.S. signals intelligence activities and for protecting the United States against hostile SIGINT.

SIGINT actually comprises several different types of intercepts. The term is often used to refer to the interception of communications between two parties, which is also known as communications intelligence (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 electronic intelligence (ELINT).

The ability to intercept communications is highly important, since it gives insight into what is being said, planned, and even considered. This is as close as one can come, from a distance, to "reading the other side's mind," a goal that cannot be achieved by imagery. Tracking communications also gives a good "indication and warning." As with imagery, COMINT relies to some degree on regular behavior by 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 the content. (*See box, "SIGINT versus IMINT," p. 66.*)

COMINT also has some weaknesses. First and foremost, it depends on there being communications that can be intercepted. If the target goes silent or opts to communicate via secure landlines rather than through the air, then the ability to undertake COMINT ceases to exist. It might be possible to tap the landlines, but this is obviously 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 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 we are far removed from the Elizabethan age of relatively simple ciphers. Computers greatly increase the ability to construct complex, one-time use codes. At the same time, computers also increase the ability to attack these same codes. Finally, the target can use false transmissions as a means of creating less compromising patterns or as a means of subsuming important communications amid a flood of meaningless ones—in effect, increasing the ratio of noise to signals.

TELINT and ELINT offer valuable information on weapons capabilities that would otherwise be unknown or would require far more risky human intelligence operations. 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. Test data 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" rather than 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 will move at irregular intervals. Receivers can be

SIGINT versus IMINT

A director of the National Security Agency once made the following distinction between imagery and signals intelligence: "IMINT tells you what has happened; SIGINT tells you what will happen."

It is a bit of an exaggeration—and was said tongue in cheek—but it captures an important difference between the two INTs.

programmed to match the frequency changes, but this will greatly increase the difficulty of intercepting the full data stream.

MEASUREMENT AND SIGNATURES INTELLIGENCE. TELINT and ELINT are both major contributors to a little understood branch of intelligence known as measurement and signatures intelligence (MASINT). This type of intelligence refers to weapons capabilities and industrial activities. Multispectral and hyperspectral imagery (MSI and HSI), discussed above, 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 increasing importance. For example, MASINT can help identify the types of gases or waste leaving a factory, which can be extremely important in chemical weapons identification. It can also help identify other specific characteristics (composition, material content) of weapons systems.

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 with it—and probably less comfortable—than they are with IMINT or SIGINT.

HUMAN INTELLIGENCE HUMINT is espionage—spying—and is sometimes referred to as the world's second-oldest profession. It is as old as the Bible. Joshua sent two 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 famous spies from history such as Nathan Hale or Mata Hari (both failures) or the many fictional spies such as James Bond. In the United States HUMINT is largely the responsibility of the CIA, through its Directorate of Operations (DO). DIA also has a HUMINT capability with the Defense HUMINT Service (DHS).

HUMINT largely involves sending agents to foreign countries where they attempt to recruit foreign nationals to spy. Agents must identify individuals who have access to the information that we may desire; gain their confidence and assess their weaknesses and susceptibility to being recruited; and make a "pitch" to them suggesting a relationship. Sources may accept a pitch for a variety of reasons: money, disaffection with their own government, blackmail, thrills. Once the pitch has been accepted, the agent must meet with his or her sources regularly to receive information, holding meetings in such a way and in such places so as not to be caught and then transmitting the information back home.

In addition to gaining the skills required for this activity, agents 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. Agents with official cover hold another government job, usually posted out of 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 (called NOC—pronounced "knock") avoids any overt connection between the agent and his or her government but can make it more difficult to keep in contact.

In addition to recruiting foreign nationals, HUMINT agents 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 involves more than just espionage.

Espionage provides a very small part of the intelligence that is collected. IMINT 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 also may offer opportunities to influence that government by feeding it false or deceptive information. For intelligence targets where the technical infrastructure may be irrelevant as a fruitful target—such as terrorism, narcotics, or international crime, where

the "signature" of activities is rather small—HUMINT may be the only available source.

HUMINT also has disadvantages. First, it cannot be done remotely, as the various types of technical collection can be. It requires proximity and access and therefore must contend with the counterintelligence capabilities of the other side. It is also far riskier, since it puts individuals at risk, and, if they are caught, has 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 spies need to build successful cover stories.

Like all the other collection INTs, HUMINT is susceptible to deception. Some critics argue that HUMINT is the most susceptible to deception. The "bona fides" of human sources will always be subject to question initially and, in some cases, may never be wholly resolved. Many questions will arise and linger. Why is this person offering to pass information—ideology, money, vengeance? Of course, he or she 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," that is, 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 will be collecting information on your HUMINT techniques and capabilities even as he or she passes information to you?

HUMINT agents must walk a fine line between prudent caution and the possibility that too much caution will lead them to deter or reject a promising HUMINT source. Deception is particularly difficult to deal with, because people naturally find it difficult to accept the fact that they are being deceived. On the other hand, people might slip into a position where they trust no one, which can result in turning away sources who might have been very valuable.

Another issue to be considered with HUMINT is its unique sources and methods. HUMINT sources are considered to be extremely fragile, since 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 told, for example, "this report comes from a first secretary in the Fredonian Foreign Ministry." Instead, the report will include information on the access of the source, 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 have a full appreciation of the value of the source and the information.

In the United States there is constant tension 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 in 1979 and the unexpected Indian nuclear tests in 1998, also lead to demands for more HUMINT.

Again, there is no "right balance" between HUMINT and the other collection disciplines. Indeed, 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 will make an equal or even similar contribution to every issue. Clearly, it is better to have a collection system that is strong and flexible and can be modulated to the intelligence requirement at hand than to have one that swings between apparently opposed fashions of technical and human collection.

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 discussed in chapter 1 that intelligence must inevitably be about secrets. A great deal of intelligence is about secrets, but not to the exclusion of openly available information. As noted above, 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, speeches
- Professional and academic: conferences, symposia, professional associations, academic papers, and experts

One of the hallmarks of the post-cold war world is the increase in the availability of OSINT. In the post-cold war period 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" have decreased dramatically. Some 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. It is readily available, although it still requires collection. OSINT requires 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 so as to deceive than the other INTs. OSINT is also useful for helping put the secret information into a wider context, which can be extremely valuable.

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.

Popular misconceptions about OSINT, even within the intelligence community, persist. OSINT is not free. Buying print media costs the intelligence community money, as does a variety of services that are useful—if not essential—to help analysts manage, sort, and sift large amounts of data more efficiently. Another misconception is that the Internet is the main fount of OSINT. Experienced intelligence practitioners discover that the Internet—meaning searches among various sites—yields no more than 3–5 percent of the total OSINT "take."

Despite the fact that 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 the United States's national security needs could be largely met with OSINT, then the intelligence community would look very different. Some people in the intelligence community 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 the fact 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 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 would be seen as ludicrous with any other INT. This is unfortunate, since 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 where such means were really needed. Thus, properly used, OSINT could be a very good intelligence collection resource manager.

PIZZINT: Some Intelligence Humor

In addition to IMINT, SIGINT, HUMINT, OSINT, and MASINT, intelligence officers, in their lighter moments, speak of some other INTs. One of the most famous is PIZZINT—pizza intelligence. This refers to the belief that Soviet officials based in Washington would keep watch for large numbers of pizza delivery trucks going late in the evening to the CIA, the White House, the Defense Department, and the State Department as an indication that a crisis was brewing somewhere. The notion was that they would see numerous pizza trucks making deliveries and then hurry back to the Soviet embassy to alert Moscow that something must be going on somewhere.

Some other INTs that intelligence officers talk about with tongue firmly in cheek are:

LAVINT: I heard it in the men's room (lavatory intelligence).
RUMINT: rumor.
REVINT: revelation intelligence.
DIVINT: divine intelligence.

COLLECTION—CONCLUSION

Each collection discipline offers unique advantages that are well-suited to some types of intelligence requirements but brings with it certain disadvantages as well. *(See Figure 5-1, "A Comparison of the Collection Disciplines," p. 72.)* By deploying a broad and varied array of collection techniques, the United States derives two advantages: it is able to exploit the advantages of each type of INT, which, ideally, will compensate for the shortcomings of the others; 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, the absence of any overwhelming strategic threat makes the cost of collection systems more difficult to justify, and it leads some to question whether the United States needs the same level of collection capability that it did during the cold war. On the one hand, the threat to U.S. national security has greatly

FIGURE 5-1 A Comparison of the Collection Disciplines

INT	Advantages	Disadvantages
IMINT	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 in time; 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

diminished. On the other hand, the problems that remain are more diverse and diffuse to collect against than was the largely unitary Soviet problem. Ultimately, there is no yardstick for measuring national security problems against a collection array in order to determine how much collection is enough.

KEY TERMS

all-source intelligence
collection disciplines
communications intelligence (COMINT)
cryptographers
deception
denial
denied areas
denied targets
electronic intelligence (ELINT)
encryption
espionage
geosynchronous orbit
human intelligence (HUMINT)
imagery intelligence (IMINT)
indications and warning
INTs
measurement and signatures intelligence (MASINT)
negation search
noise versus signals
nonofficial cover (NOC)
official cover
open-source intelligence (OSINT)
photo intelligence (PHOTINT)
pitch
resolution
signals intelligence (SIGINT)
sources and methods
spies
telemetry intelligence (TELINT)
traffic analysis
wheat versus chaff

FURTHER READINGS

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

General Sources on Collection

Burrows, William. *Deep Black: Space Espionage and National Security.* New York: Random House, 1986.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision.* Stanford, Calif.: Stanford University Press, 1962.

Espionage

Burgstaller, Eugen F. "Human Collection Requirements in the 1980's." In *Intelligence Requirements for the 1980's: Clandestine Collection,* edited by Roy F. Godson. Washington, D.C.: National Strategy Information Center, 1982.

Phillips, David Atlee. *Careers in Secret Operations: How to Be a Federal Intelligence Officer.* Frederick, Md.: Stone Trail Press, 1984.