Chapter 5
Information and Context

Security Analysis Critical-Thinking Framework

Bottom Line Up Front

Searching for information and developing the context for a professional or academic critical-thinking project is often a daunting task. Searching for information may take the most time of any of the critical-thinking elements. It requires that analysts master the skills of information literacy, including establishing information needs, locating and evaluating information, and effectively using the information in their analyses. There are an abundance of sources for information. Government-run intelligence systems provide both collected raw information and finished intelligence products, which are available to analysts with security clearances. All analysts may access unclassified, open-source material available to the general public—information that makes up a significant part of strategic analytic products. At times, analysts find they must collect their own information using social science data-collection methods. Information located must be assessed for its validity. In a nutshell, analysts must

become both their own reference librarian and a "critical consumer of information."

A Mountain of Information

Finding and assessing **information** will likely be the most time-consuming part of any analytic project. In today's Information Age, analysts must digest a mountain of information—sometimes characterized as "drinking from a fire hose." Analysts are normally assigned a **portfolio**, meaning a specific regional or functional area of analytic focus. A portfolio for both security analyst practitioners and academics may cover a geographic region, specific state, and/or functional areas such as terrorism, drug trafficking, immigration, weapons proliferation, weapons technologies, military planning, or other areas supporting the national and homeland security communities. Within their assigned portfolio, analysts must understand the historical, political, economic, military, social, cultural, and technological aspects of their analytic area. Knowing this background allows the analyst to develop an understanding of the **context** of situations, which includes the historical, political, economic, military, and social background on a situation. At first this may seem like a gargantuan effort, but the analyst will normally have considerable help in completing these tasks. Practitioner and academic communities employ a number of library resources, databases, daily messages, and other resources to assist analysts in climbing their particular information mountain. Other analysts usually are available to assist in research.

Analysts do not normally start their information quests from scratch. Many possess an academic degree related to their portfolio. Additional local classroom and online college courses related to the analyst's portfolio may be available to assist in knowledge acquisition. Professional training courses on specific aspects of the analyst's portfolio also may be available. As analysts gain knowledge and experience, they will also develop a deeper understanding of the context of their portfolio. Most analysts develop a personal reading program to help build their

portfolio expertise. This may include reading reports from other agencies and digesting the daily avalanche of messages containing the latest reporting. It may include regular reading of multiple information sources described in this chapter. Regional and state analysts normally will read a select list of online or paper versions of newspapers and magazines from their region or state. This may require analysts to develop reading proficiency in the languages of their assigned region or state. Analysts also will gain information in intra-agency and interagency meetings or in professional and academic conferences. Information search efforts must be coordinated with the analyst's production schedule of written and verbal reports. Additionally, analysts also should devote time to improving their expertise on the latest analytic methods and techniques applicable to their portfolios. It should be obvious that analysts must develop strong work ethics and good time management skills.

Assistance to analysts also will include working in analytic teams. It is unlikely one analyst can comprehend all the information related to specific research question(s); therefore, analytic teams provide the best approach to understanding the breadth of background information on a situation and allow a number of perspectives to be applied to the analysis. Analytic teams at larger agencies may include specialists in political science, economics, sociology, anthropology, psychology, military studies, and/or technical aspects of the particular project. The Cuban Missile Crisis case study presented in Box 2.1 describes how President Kennedy expanded his team of advisors with Cuban and Soviet specialists and others who could provide alternative perspectives as he developed his plan of action.

Whether analytic teams are employed depends on the timeline and topic of the analysis to be conducted. In a larger **strategic analysis** project, analytic teams are commonly used. Strategic analysis is usually less time-sensitive and includes "big picture" studies that may result in book-length final reports. For example, a study of the North Korean military threat to South Korea would be a strategic analysis. For more time-sensitive, **operational analysis** or **tactical analysis**

projects, it is likely one or two analysts will work on the project, but other analysts may assist as needed. Operational and tactical analysis reports are usually on current events that support ongoing or future operations and may range from several pages to just a few paragraphs. Agencies often have differing definitions of operational and tactical analysis. One way to differentiate the two is to think of operational analysis as being when the general behavioral trends of adversaries are known, but little is known about their exact locations or near-term intentions. The operational analysis then would focus the analytic effort on developing the potential threat and the adversaries' best alternatives for employment of operational forces or other resources. Tactical analyses are conducted when there is information on the locations and likely intentions of an adversary, so that more-refined alternatives can be developed for the employment of friendly operational forces or other friendly resources.

The information search on an analytic project never ends. The Security Analysis Critical-Thinking Framework diagram at the beginning of this chapter indicates that there are two main phases for the information element. In the first phase, the analysts uncover what is already known on a topic; then, after completing the conceptual element of the framework, a second phase is instituted to fill information gaps with data to test hypotheses or otherwise complete the analysis. The context element in critical thinking applies to every element; but, in particular, to the information element as the context is established through analysis of acquired information. The information element also applies to all elements because additional information likely will be needed as each element in the framework is addressed. As the finishing touches are made to any written or verbal report, the information search continues to ensure the latest information is included in the analytic reports presented to customers.

Information literacy is a skill all analysts must master. Information literacy is the ability to recognize the extent and nature of an information need; then to locate, evaluate, and effectively use the information. Once the analytic project's purpose and specific research question(s) are developed (Chapter 4), the next

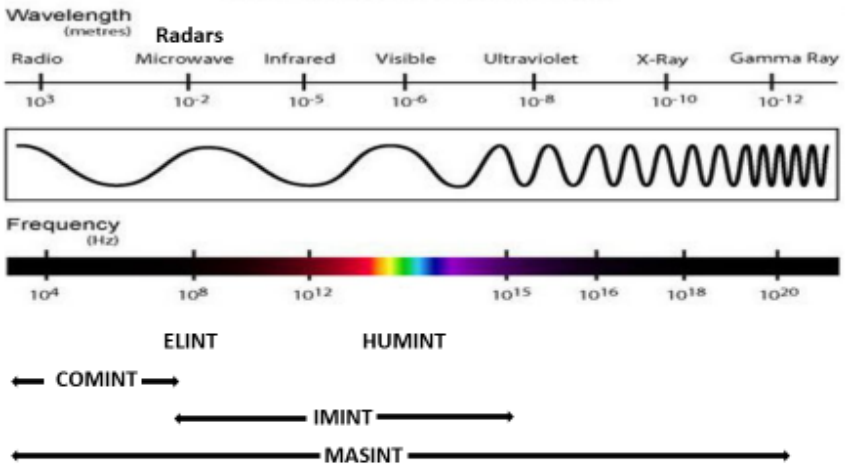
step is to employ information literacy skills to determine the availability and quality of existing information to answer the specific research question(s). This chapter provides a roadmap for developing this skill as well as guidance on locating and evaluating information. In security analysis, the information may be available from government **intelligence collection** systems accessible to practitioners and academics with security clearances. Although the U.S. Intelligence Community (IC) maintains these collection systems, analysts with proper clearances may have access to both **raw information** gathered from these systems and the **finished intelligence reports** produced from the collection efforts. All analysts normally have access to unclassified information available through a variety of sources—today called **open-source intelligence (OSINT)** in government circles. At other times, analysts may find a need to conduct their own information collection using social science data-collection methods. Classified IC collection results, unclassified material available to a wider audience, and analyst self-collected information may all include significant biases. This chapter introduces both the classified and unclassified resources that security analysts may have available as they search for and assess information. It also discusses potential biases in this information. How best to use that information will be covered in subsequent chapters.

Note: Many analytic projects go off-track early due to a failure to focus the information search on the specific research question(s). Time constraints normally do not allow the analysts to make a broader search beyond the specific research question(s). Failure to focus the information search may result in information gaps and inabilities to meet written or verbal reporting production deadlines. Time management is key!

Intelligence Information

Government-run intelligence-collection systems cost billions of dollars each year and are the foundation of much of the information utilized by security practitioners. The systems range from networks of human agents to extremely expensive technical collection conducted by shore installations, ships, aircraft, and satellite-based systems. Technical collection makes use of the United States' advanced scientific and technical abilities to exploit physics, chemistry, and biology, including the electromagnetic spectrum. As diagrammed in Figure 5.1, the electromagnetic spectrum ranges from low-frequency radio waves to high-frequency gamma rays, including microwave (radar), infrared, visible light, ultraviolet, and x-ray signals. Figure 5.1 also notes the various intelligence-collection disciplines (more on those below) that exploit portions of the electromagnetic spectrum. Both the raw information and finished intelligence produced by and from human and technical collection is largely classified for two reasons. First, to deny adversaries knowledge of what is known about them. Second, to protect the sources and methods used in gaining the raw information and producing the finished intelligence.

Figure 5.1 The Electromagnetic Spectrum



Intelligence-collection systems usually are discussed in terms of **collection disciplines**, commonly labeled **INTs**. As explained below, national security collection is coordinated by specific national security agencies. Federal law enforcement collection is directed by the individual collecting agency and is coordinated with other national security agencies as needed. State and local Homeland Security Fusion Centers play a unique role, as they arrange for national collection support to state and local agencies, and also coordinate the flow of raw information and finished intelligence among national security agencies, federal law enforcement agencies, and state and local law enforcement. Although security analysts should have a deep understanding of the collection disciplines, that is beyond the scope of this book. This chapter does; however, provide a general introduction to the disciplines and discusses strengths, weaknesses, and potential biases inherent in each. To gain a deeper understanding of intelligence collection, security analysts should read Robert Clark's *Intelligence Collection*,[1] and then expand their knowledge of collection through additional reading and visits with the actual collectors most used to support their portfolio analysis.

One goal of the IC is to combine information gleaned from several different collection disciplines; i.e., multiple INTs, at federal, state, and local levels and produce **all-source intelligence** reports. This assumes that agencies responsible for the various collection disciplines and collection programs actually share the information collected. This is not always the case. In the September 11, 2001, *al Qaeda* terrorist attacks on the United States, several agencies had partial information on the terrorists and their intentions. *The 9/11 Commission Report* uncovered how the information was not properly shared, contributing to the death of 2,977 people in the New York World Trade Center, Pentagon, and the four airliners used as *ad hoc* missiles in the attacks.[2] The lack of information sharing adds significant bias to analytic reports when all-source analysts simply do not have the information needed to "connect the dots."

Another significant bias in intelligence collection is **selection bias**. Even with billions of dollars spent annually on intelligence-collection systems, they cannot

collect and process information on everything in the world. Therefore, collection efforts must concentrate on the highest priorities. This creates an upfront selection bias as the bureaucratic institutions decide what information will or will not be collected. In the United States, national-level intelligence-collection priorities are developed through interagency collection plans coordinated through the Office of the Director of National Intelligence (ODNI). These plans are approved by the National Security Council (NSC) process. The national-level collection plans are turned into *standing collection requirements* and then sent to various agencies assigned to build, operate, and maintain specific collection systems. Most INTs primarily collect against and report on national-level standing collection requirements; however, to ensure responsiveness to operational and tactical intelligence needs, most military commanders and large law enforcement field agencies have their own collection capabilities. Agencies may request alterations or additions to national-level standing collection requirements to assist in specific analytic projects. The requesting agency must submit a *focused collection requirement*, which is then vetted through an interagency process; and, if approved, will allow the re-tasking of intelligence-collection systems. This may sound like a bureaucratic barrier; but, in reality, requests to re-task intelligence-collection systems are a common and usually timely occurrence—but not always. A common problem among security analysts is their failure to know enough about intelligence-collection systems and how and when to submit focused collection requirements.

Human intelligence (HUMINT). This is a general term used for an eclectic group of collection activities where information is usually gathered from humans by human collectors. HUMINT activities stretch back centuries. *The Bible* records how around 1445 BCE, Moses sent "men to spy out the land of Canaan" in order to scout their defenses.[3] In today's context, HUMINT includes clandestine collection (often called espionage or spying), overt collection, interrogation, and foreign liaison activities. Primarily a non-technical means of collection, HUMINT is

the least expensive of the INTs. The Central Intelligence Agency's (CIA's) Directorate of Operations (DO) oversees national security HUMINT collection efforts to ensure those collection activities are coordinated and de-conflicted. Federal law enforcement agencies have their own HUMINT assets used in both domestic and foreign collection. Law enforcement foreign HUMINT collection activities normally support U.S.-based investigations.

Clandestine HUMINT. The collection of information by clandestine means, and sometimes corresponding covert actions, are the sensationalized subject of spy tales in novels, movies, and television programs. This dramatic Hollywoodesque-view of espionage is far from the norm. National security HUMINT clandestine collectors are called **case officers**. Their main job is to develop sources through a step-by-step process of spotting, evaluating, recruiting, testing, training, and handling human sources.[4] Using this process, it may take months, if not years, to spot and evaluate prospective recruits leading to their becoming productive clandestine sources.

HUMINT spotting activities. Entail identifying individuals that may be susceptible to recruitment and who have access to the information the collector wants. Individuals of interest as possible recruits span a range of accesses from high-level government and military officials to staff who work for such officials or work in the same buildings as these officials. It also includes business persons or others who have knowledge of or access to what the collector wants. A main goal of national security HUMINT collection is to obtain planning documents, technical manuals, contingency plans, and weapons-systems blueprints.[5] Sometimes potential recruits are "walk-ins," meaning they seek out HUMINT collectors and readily volunteer their services. Other potential recruits require significant collector effort to spot, evaluate, and recruit.

HUMINT evaluation activities. Entail case officers identifying the motivations and personal characteristics of a potential recruit. This allows case officers to determine if they can use the recruit as a unwitting source (see overt HUMINT collection below) or if it is worth taking steps to recruit the person to voluntarily agree to provide information to the case officer. In coordination with supervisors, the case officer then decides if the timing is right to recruit the individual. The case officer or another clandestine recruiter will usually make the approach on the recruit. Once a recruit voluntarily agrees to work for the case officer, he/she is then tested to determine their actual access to information. If they pass the testing, they are then trained by the case officer in clandestine "tradecraft," including how they will communicate with the case officer. Once training is complete, the collection activities of the new source will be managed by the case officer. For the information they provide, clandestine sources are usually compensated with money or other items of value (visas, asylum, etc.). Law enforcement recruiters utilize a similar step-by-step process to recruit clandestine "informants" who provide HUMINT to support U.S. domestic and foreign investigations.

When carried out in foreign states, clandestine HUMINT activities may be illegal because state espionage laws may be violated if a clandestine collector attempts to recruit government or military officials. When clandestine activities include **covert actions**, such as "surreptitious entry" (breaking and entering), that also violates state laws. A covert action is any activity where the sponsor of the activity (i.e., the U.S. government) is meant to be kept secret and, in most cases, to ensure the activity itself is never detected. HUMINT collectors continually assess the "risk versus gain" of their collection activities and covert actions. Risks include how an activity gone awry would affect the case officer, source, or the United States. Gain refers to the expected amount and quality of the information to be collected. To protect the clandestine case officers from foreign-state

criminal prosecution, they normally work as an employee of a U.S. government agency located in the foreign state and are given diplomatic immunity. These individuals are usually protected from foreign-state prosecution but not from deportation after being declared a "*persona non grata.*" Diplomatic immunity is part of an international game all states play, recognizing foreign government personnel working in a state may be protected from criminal prosecution. There are even more critical risk calculations when the clandestine collector is placed in a foreign state in a non-official cover (NOC) status without diplomatic immunity. Working as journalists, business officials, or other positions to facilitate access to information, if a NOC collector is caught in an illegal activity, he/she can be prosecuted and imprisoned in the foreign state. NOC collectors must be extremely cautious not to reveal their connections to the IC.

Overt HUMINT. Overt collection includes a number of activities such as interviews, elicitation, observation, and handheld photography. Overt collectors may be State Department officials, defense attachés, or other U.S. government personnel in the U.S. Embassy or governmental organizations that target unwitting sources and report any relevant information to their home agencies. Clandestine case officers are also involved in overt collection from unwitting sources. Overt collectors often will interview senior and mid-level host-state government, military, or business officials and report the interview results to their home-state agencies (including to the IC). Overt IC national security collectors are trained in elicitation, the ability to engage unwitting sources in conversations in such a way that the collector gathers the information they seek while the source remains unaware of the elicitation. Overt collectors also observe activities in the foreign state by attending official ceremonies and social functions where they have access to senior government and military officials. Observation also is conducted during visits to military installations and businesses. Observations, interviews, and elicitation of unwitting sources also may be conducted at professional, scientific, and technical conferences. HUMINT observations often

are combined with information from interviews and elicitation to strengthen intelligence reporting. Overt HUMINT collectors are often trained in handheld photography to supplement their reporting and provide ground truth to support **imagery intelligence (IMINT)** activities discussed below. Overt HUMINT collectors usually have diplomatic immunity, although their activities do not normally cross the line of being illegal in the foreign state.

Interrogations. Another HUMINT activity entails interviewing subjects in controlled situations. Migrants who cross foreign borders from a denied area, such as North Korea, Cuba, etc., may be interrogated by U.S government officials to determine their access to information and inquire about their personal observations in their home state. For example, Cuban migrants arriving in South Florida provided the first indications the Soviets were installing nuclear missiles in Cuba—leading the IC to re-focus and expand collection efforts on Cuba before the 1962 Cuban Missile Crisis (see Box 2.1). During war or other conflicts, CIA and military interrogators may question detainees and prisoners-of-war. The United States came under domestic and international condemnation for its interrogation activities made public during the early-21st century wars in Iraq and Afghanistan and in the War on Terror after the September 11, 2001, attacks on the U.S. homeland. In 2009, this led President Obama to sign an executive order directing that all U.S. federal agencies follow the interrogation policy and procedures in *U.S. Army Field Manual 2-22.3 Human Intelligence Collection Operations*[6] in all interrogation operations. This field manual prohibits enhanced interrogation techniques that cause extreme physical or mental distress and torture including waterboarding, physical injury, and other techniques. After detention or arrest in domestic situations, interrogations often are conducted by law enforcement agencies. Federal law enforcement agencies also must follow the *Army Field Manual* guidance and U.S. privacy laws.

Foreign liaison. Working with foreign governments can provide a

substantial amount of HUMINT reporting. U.S. intelligence agencies frequently establish liaison relationships with their foreign counterparts and may share both raw information and finished intelligence. One key U.S. foreign liaison program is dubbed the "Five-Eyes" with member states the United States, United Kingdom, Canada, Australia, and New Zealand. These allies share intelligence collection and analytic products. Outside the Five-Eyes structure, most U.S. intelligence liaison between states is based on a *quid pro quo* approach, either formally established or just confirmed by verbal or hand-shake agreements. Alternatively, the U.S. may provide a foreign liaison partner with case-specific information or other resources in exchange for information generated by the partner's intelligence programs. Such liaison is usually conducted with friendly or allied states. An example of foreign liaison relationships, during the 1962 Cuban Missile Crisis (see Box 2.1) was with the United Kingdom. They provided the United States information from one of their HUMINT sources, Soviet Army Lieutenant Colonel Oleg Penkovsky, who reported the Soviet missiles in Cuba were not operational and the overall Soviet nuclear arsenal was not as large as the West estimated. This liaison-provided information allowed President Kennedy to be more aggressive in his decision making.

HUMINT strengths. HUMINT is not as expensive as the technical intelligence collection disciplines and is especially useful for directing technical discipline collection. Most importantly, it can provide the intentions of adversaries. HUMINT expenses include recruiting and training personnel, paying personnel, ensuring collectors have office space and staff support, providing foreign housing (if needed); and purchasing collection support equipment (i.e., cameras, communications, etc.). Some HUMINT collectors also have access to their own aircraft for use in moving more easily within a foreign state or region.

A single HUMINT report or source usually is not the only information in finished intelligence reports; however, a HUMINT report can be the key to employing other collection disciplines against a collection requirement. Each

HUMINT report should be verified and coordinated with other HUMINT reporting and information collected by one or more of the technical collection INTs discussed below. For example, a HUMINT report gained through foreign liaison may indicate a specific vessel is preparing to smuggle drugs from a foreign state to the United States. Working with a foreign liaison partner, the U.S. may request the foreign-state police to seize the vessel and arrest the crew before it leaves the foreign state. If this is not the case, the foreign liaison partner and U.S. HUMINT collectors may surveil the vessel allowing notification of the IC and U.S. counter-narcotics forces of its departure from the foreign state. U.S. technical collection disciplines, such as imagery intelligence (IMINT), communications intelligence (COMINT), and surveillance forces could be focused on the vessel's departure point and along its track in order to vector in counter-narcotics forces to seize the vessel and arrest the crew.

HUMINT's main strength is its ability to determine the intentions of adversary states. Among the technical collection disciplines, usually only COMINT and cyber intelligence collection can help determine intentions. For example, obtaining copies of a foreign state's planning documents and contingency plans could provide their intentions. HUMINT collection also can penetrate denial operations. For example, a foreign state may be planning to deploy a new military capability. This state may have reasons to keep this new military capability undisclosed (denied) to other states until its deployment is completed. HUMINT collection is likely the only source able to collect information on the new military capability through collector access to the foreign state's military or other government officials.

HUMINT weaknesses and potential biases. HUMINT has a number of weaknesses that may add significant biases in reporting. HUMINT usually cannot be conducted remotely, because HUMINT collectors usually meet face-to-face with their sources (informants) during the clandestine spotting, evaluating, recruiting, testing, and training steps, or when overt collectors meet with

government, military, or business officials. When the source is intended to provide information on activities such as terrorism, drug smuggling, or other organized crime, the HUMINT collector may have to meet and interact with unsavory characters. Most foreign states, large terrorist organizations, and organized crime syndicates frequently employ counterintelligence personnel to specifically look for espionage or other spying activities. Thus, HUMINT planning must consider the "risk versus gain" before HUMINT collectors go forward with face-to-face collection activities.

The biggest source of HUMINT bias is collection and reporting of **misinformation**, which is mistaken or deliberate false or inaccurate reporting. This bias can have a number of origins, including sources who may be opportunistic, a motivation not uncovered in the recruiting process. Opportunists provide misinformation as they seek money or other items of value. Eventually the opportunist will be uncovered, but not before they have done major damage. HUMINT collectors also must be aware of overt opportunists, or sources who provide misinformation to bolster their egos and self-importance in the presence of government or military officials. One of the most noted HUMINT opportunists was a source dubbed "Curveball," who provided misinformation on Iraqi weapons of mass destruction (WMD) programs that contributed to the U.S. 2003 invasion of Iraq. See Box 5.1 for additional information on Curveball. HUMINT derived from interrogations also may be biased when the source provides the interrogator information the source thinks the interrogator wants to hear in order to end the interrogation. According to the U.S. Senate Select Committee on Intelligence in their "Study of the CIA's Detention and Interrogation Program," such misinformation often resulted from use of enhanced interrogation techniques or torture.[7] More recent interrogations conducted within the policy of *U.S. Army Field Manual 2-22.3* still may result in misinformation because the source wants to end the interrogation. The *Army Field Manual* does authorize a number of emotional and physical interrogation approaches, short of torture, to make the source mentally or physically uncomfortable. This also may lead the source to

provide misinformation to end any discomfort or pain. Employment of "dangles" may also provide misinformation and bias to HUMINT reporting. A dangle is when a state or criminal organization puts forth a HUMINT source to purposely feed misinformation into HUMINT reporting. This is usually part of a larger deception plan (see discussion of deception below).

Box 5.1 Curveball: HUMINT Con Man[8]

Rafid Ahmed Alwan, U.S. codename "Curveball," was an Iraqi citizen who studied chemical engineering at the university level. In November 1999, he defected from Iraq to Germany and requested political asylum. He claimed he had worked as a chemical engineer at an Iraqi plant that manufactured mobile, biological-weapon laboratories as part of Iraq's WMD program. He was debriefed by German intelligence from December 1999 to September 2001. His debriefing reports were provided to the U.S. IC through foreign liaison channels with German and British intelligence services. Both intelligence services questioned the validity of Curveball's information.

In 2002, the U.S. NSC requested the CIA produce an assessment of Iraqi WMD programs. Working on a short deadline and with sketchy information, in October 2002, the CIA's National Intelligence Council (NIC) published a National Intelligence Estimate (NIE) on Iraqi WMD.[9] During the NIE's writing, Bush administration policy staffers (including Vice President Richard B. Cheney) engaged directly with the intelligence analysts to guide the NIE analysis, ensuring the report supported already-planned U.S. actions. The NIE, which inaccurately predicted the existence of Iraqi WMD, was used as a key component of the justification for the 2003 U.S. invasion of Iraq. Later investigations found the NIE placed too much credence on one unreliable source (i.e., Curveball). Investigators also found the analysis lacked robustness, and its findings were based on faulty assumptions.[10]

U.S. intelligence was not given direct access to Curveball before the October 2002 NIE. Only after the 2003 Iraq invasion was it confirmed that Curveball had fabricated the entire story about Iraqi biological weapons. To keep Curveball talking during his debriefings, he was granted political asylum in Germany. He requested resettlement (similar to U.S. witness protection), including requests for a big house and a Mercedes automobile. He also wanted an engineering job—even though he did not speak German and made little effort to learn the language. He requested arrangements be made to bring his wife and parents from Iraq to Germany. He turned out to be a classic opportunistic HUMINT source who provided misinformation in exchange for his resettlement in Germany. His wife did join him in Germany in 2004 where they had a daughter. He was granted German citizenship and, by 2010, was still under German police protection. He remained bitter about German failure to meet all his resettlement demands; in particular, about not getting a German engineering job. In 2004, U.S. intelligence interrogators finally gained access to Curveball. Even though U.S. interrogators pointed out inconsistencies in his original debriefings with what U.S. forces found in Iraq, Curveball never recanted his story about Iraqi biological weapons.

Another source of bias in HUMINT reporting is from the collectors, who as humans possess inherent biases. Clandestine case officers are usually specialists in the states or regions where they work. They usually speak the state or region's languages and are well trained in clandestine tradecraft. The same may not be true of overt collectors. Some overt collectors are specialists in their state or region, speak the languages, and are well trained in tradecraft; others may be part-time collectors and are not necessarily fully prepared for their collection role. For example, State Department Foreign Service Officers, who are the Department's main reporters, often move between world regions in assignments

and may not be specialists in host-state politics, economics, etc., where their overt reporting concentrates. Defense attachés are senior or mid-level officers with military specialties. They also may be new to the host state or region, have only basic foreign language skills, or not be intelligence specialists. Exceptions include defense attachés who are intelligence specialists or military Foreign Area Officers (FAOs) who are well trained, fluent in local languages, and experienced in their host state or region. Another type of selection bias occurs when HUMINT collectors only report a small amount of what they collect. It is estimated some collectors may only have time to report 10-15% of what they actually know on a topic. This is why it is important for analysts to submit *Requests For Information* (RFIs) to collectors in order to fill intelligence gaps or tell the "rest of the story" on HUMINT reporting. Finally, HUMINT collectors may become advocates for their host state in their reporting instead of providing more-balanced and objective reporting. The opposite also is true when the HUMINT collector has a cynical view of the host state and taints his/her reporting with negative information. As can be seen from the above discussion, there are many potential biases that can creep into HUMINT reporting.

Signals intelligence (SIGINT). Is a traditional umbrella term for two separate technical collection disciplines—**electronic intelligence (ELINT)** and **communications intelligence (COMINT)**. The lead agency for U.S. national security SIGINT collection is the National Security Agency (NSA), a subordinate unit of the U.S. Department of Defense. In addition to overseeing its own SIGINT collection and that of other U.S. military services, through its Central Security Service, NSA also provides all communications encryption devices and codes to the U.S. military and other government agencies. Federal law enforcement does not collect ELINT, but its foreign COMINT activities usually are coordinated by NSA or the Federal Bureau of Investigation (FBI). NSA also houses U.S. Cyber Command, which is discussed in more detail below in the Cyber intelligence section.

Electronic intelligence (ELINT). Applicable mainly to military operations, **ELINT** is collection of signature data from microwave radar (**Ra**dio **D**etection **a**nd **R**anging) equipment. Radar was invented in the late-19th century where radio waves were used to detect distant metal objects. Radar did not become widespread until World War II when it was deployed by both Allied and Axis forces. Today, radar is used extensively to detect both military and commercial ships and aircraft, for maritime and air navigation, and for detecting weather phenomena.

ELINT collectors from permanent and mobile land-based units, ships, aircraft, and satellites collect radar signature data from both military and commercial radar systems worldwide. Radar signatures include signal strengths, radar frequencies, pulse widths, and pulse-repetition frequencies. With this data, a military unit can determine the type and location of a radar and, from database information, determine the type of ship, aircraft, or land-based unit. From the radar signature, the collector may determine the use of the detected radar such as for navigation, area search, targeting, or weapons control. This allows military units to evaluate the existence of a potential threat before the threat is in visual sight or located on the unit's own radar systems.

NSA oversees the collection of ELINT data and maintains the databases used to catalog the data. NSA issues the database information to military units with **Electronic Support Measures (ESM)** equipment for detecting and classifying radar signals. In addition to the detection and classification of radars, ELINT allows a military tactical commander to avoid radars or to jam any known radar frequencies in order to deny their use to adversaries.

ELINT strengths and weaknesses. ELINT's main strength is the ability to detect adversarial radar systems and evaluate the existence of threats at greater distances than the ELINT collector's own radars or other sensors. ELINT's main weakness is its susceptibility to denial and deception operations. To deny U.S.

detection of radar signals, an adversary can use **Emission Control (EMCON)** to turn off their radars or use them intermittently in selective tactical modes. They also may transmit deceptive radar signals to disrupt or degrade operational or tactical use of signals. Due to its highly technical nature, ELINT is of primary use to security analysts involved in technical ELINT analysis or tactical military planning.

Communications intelligence (COMINT). NSA defines **COMINT** as "technical and intelligence information derived from foreign communications by other than their intended recipient." Domestic law enforcement could use the same definition less the word "foreign."[11] COMINT activities have been around for centuries. Prior to the emergence of electronic communications, interception of human messengers carrying dispatches or observation of visual signals (semaphore, signal flags, smoke signals, etc.) was common. Telegraph message intercepts were conducted by Union and Confederate forces in the U.S. Civil War. Once Guglielmo Marconi and others invented wireless radio in the 1890s, states were able to listen to other states' messages. By World War I, the British were intercepting German wireless radio signals, and also telephone and telegraph signals by tapping submarine (underwater) cables carrying communications to and from Germany. U.S. military intelligence learned from the British in World War I. After the war, the U.S. Army and State Department coordinated what became known as "The Black Chamber" to decrypt telegraphic diplomatic and military messages. World War II saw an expansion of COMINT operations, including the interception, decryption, and direction finding of medium- and high-frequency wireless radio signals. For example, during the World War II Battle of the Atlantic, Allied forces were able to decrypt messages between units of the German Navy and—using direction finders—were able to locate German U-Boats and direct Allied antisubmarine forces to their locations.

Today, electronic communications are intercepted from landline telephones, wireless radio, and digital communications from cellular, satellite, and cable systems. Intercepted signals may include voice and data transmissions,

diplomatic and military messages, facsimiles, voice mail, videos, electronic mail, text messages, and any other mode of person-to-person communication transmitted electronically. By the 1990s, the widespread use of digital and satellite communications necessitated that NSA develop new COMINT collection capabilities to intercept mainly digital signals, instead of the analog telephone and wireless radio intercepts more common in the past. Today's COMINT collection is focused on a number of areas, including political and military leadership, military units and their operations, research and development programs, military testing facilities, criminal enterprises, and economic activities.[12] The COMINT process includes several steps.

1. There must be access to the targeted communications system, which is accomplished by intercepting open-air signals or tapping into cable systems, including gaining access through telecommunications providers.
2. The communication must be collected.
3. The communications must be processed, meaning it may have to be both decrypted by cryptologists and/or translated by language interpreters.
4. The communication must be analyzed. Three types of analysis may be conducted:

- **Content analysis** is conducted wherein the text of the intercepted messages becomes apparent through decryption and translation.
- **Traffic analysis** is when the text of the messages may not be readily available, but adversary intentions may be inferred through characteristics of the message transmitted, such as sender, time of transmission, frequency, and length of message.
- **Signature analysis** is used to generate intelligence through the actual signature of the equipment used to transmit messages and data. The most basic of signature data includes telephone numbers and Internet URLs. Additionally, all communications

equipment—even of the same model—have specific electronic signatures. Similar to ELINT, COMINT signatures can determine which unit transmitted the message and, when combined with traffic analysis, can assist the analysis even when they do not have the messages' actual contents.

5. The results of the COMINT analysis must be disseminated to customers. Decrypted, raw information intercepts may be submitted to some customers that have their own translators. Other customers may receive finished intelligence from all-source analyses where the COMINT is synthesized with information from other INTs.

Law enforcement COMINT. This collection conducted by government non-military units presents its own challenges. Foreign law enforcement COMINT usually is conducted by NSA either remotely or in a foreign state through bilateral agreements, liaison arrangements, or by U.S. collectors with diplomatic immunity. U.S. privacy laws do not apply in foreign countries unless the U.S. collection activity is on a U.S. entity (citizen, corporation, etc.) or if the signal intercepted originates or ends in U.S. territory. Domestic law enforcement COMINT requires strict compliance with U.S. privacy laws. These laws often change based on perceived immediate threats to the United States. For example, soon after the September 11, 2001, terrorist attacks on the United States, the USA Patriot Act was enacted allowing an expansion of U.S. national security and law enforcement domestic HUMINT and COMINT collection activities against potential terrorist threats on U.S. territory. Over time, the public and Congress began to object to the USA Patriot Act's expanded collection capabilities, and the activities were slowly retracted. In general, any domestic law enforcement COMINT activity (wiretaps, electronic "bugs," acoustic listening, etc.) requires a warrant obtained through the U.S. justice system. Moreover, domestic COMINT collection results must comply with U.S. privacy laws in order to be used in a criminal court case.

The exception to this domestically is national security or counterterrorism collection conducted within the United States. In these cases, a warrant normally is required in accordance with the procedures in the Foreign Intelligence Surveillance Act (FISA). Beginning in 1978, special FISA Court U.S. federal judges review and grant warrants for law enforcement to conduct collection within the United States or target U.S. entities outside the U.S. territory. The FBI and Department of Justice coordinate FISA warrant applications submitted to the FISA Court. Security analysts should be aware of the latest U.S. privacy laws for the collection and inclusion of COMINT in their projects.

COMINT strengths. The most significant strength of COMINT is the ability to collect volumes of raw data. COMINT collection often is characterized as a "vacuum-cleaner approach," sucking up huge amounts of information. While COMINT cannot collect all world communications, it does a good job collecting information when its collectors are focused on specific intelligence requirements. This strength is also a weakness as discussed below.

A second strength of COMINT, like HUMINT, is its ability to obtain the intentions of the senders of targeted communications. Planning documents and contingency plans often are transmitted through channels COMINT can collect. Additionally, orders to implement contingency plans may also be intercepted and can provide detailed information on an adversary's intentions. COMINT is a major contributor to established intelligence Indications & Warning (I&W) Problems covered in Chapter 10.

COMINT weaknesses and potential biases. Weaknesses in COMINT include its costs, the volume of data collected (also a strength as discussed above), the challenge of decrypting and translating the intercepts, and its susceptibility to denial and deception. All of these weaknesses can insert biases in COMINT information, as they can affect the validity of raw information and finished intelligence reporting. Information collected by COMINT collectors focused on

U.S. standing collection requirements is very expensive. Land stations, ships, aircraft, and satellites are expensive to build, deploy, and maintain. Thousands of personnel are required to operate the U.S. COMINT system. The results of effective COMINT collection; however, are considered well worth the cost.

The voluminous amount of COMINT information is both a strength and one of its greatest weaknesses. There are not enough cryptanalysts, translators, and analysts to process all the information collected. This situation is somewhat mitigated by using keywords to search the data collected or by focusing processing on high-priority communication channels developed through COMINT collection requirements. For example, COMINT collection on Osama Bin Laden's Inmarsat (International Maritime Satellite) telephone was key in developing intelligence on *al Qaeda* until a 1998 *Washington Times* article disclosed that the United States was monitoring the telephone. Whether a foreign military commander, terrorist leader, organized crime boss, or other adversaries, COMINT collection is facilitated by having exact telephone numbers, email addresses, or other specific details on the communications used by adversaries. Data storage is another challenge with the large volume of COMINT data collected.[13] NSA employs some of the most powerful computers in the world, but still is challenged with the storage of the vast amounts of data collected.

Sophisticated encryption systems and lack of translators in lesser-spoken world languages are additional COMINT weaknesses. Technologically advanced adversaries will have more sophisticated encryption systems for their communications. NSA decryption starts with its banks of powerful computers. Some less-sophisticated encryption systems, especially open voice communications, may still require human decryption by experienced cryptologists. NSA employs thousands of computer scientists, mathematicians, and cryptologists in its efforts to decrypt collected COMINT. Additionally, translators for all world languages are not available to the U.S. COMINT system. There are some languages spoken in only isolated regions of the world. In 2020, *The World Atlas* estimated there were 7,099 world languages, with the number

changing annually as new languages emerge and some languages become extinct. It is impossible to maintain translators in several thousand world languages. Additionally, some languages have dialects that differ substantially from the base language. When an adversary can employ a less-known language or dialect, it makes their communications more secure. For example, in World War II, the U.S. Marine Corps in the Pacific Theatre made use of "Navajo Code Talkers," as the Navajo language, spoken only in the southwestern U.S., was completely unknown to Japanese translators. Thus, the challenge of both sophisticated encryption systems and less-known world languages and dialects can be a huge challenge for COMINT.

As with ELINT, COMINT collection is susceptible to denial and deception. Encryption of communications is a form of denial because it hides the textual content of messages. Additionally, adversaries may use EMCON and not communicate using normal channels. When denial operations are in effect, it negates the effectiveness of COMINT. Adversaries also may generate false communications to deceive opponents as to the true operations planned or under way. For example, in World War II, Allied forces created a false set of communications signals to convince the listening Germans that a potential Allied invasion of France was targeted on the Calais region adjacent to the narrowest part of the English Channel. They even provided false commercial radio broadcasts by the fake Allied force commander, U.S. General George S. Patton, who made frequent radio speeches to various English community groups discussing the upcoming invasion—all faked to deceive the Germans. This led the Germans to concentrate their intelligence collection on southeastern England and deploy their strongest defenses around Calais. Instead, the Allies were preparing for the invasion in southwestern England and landed farther south in Normandy where German forces were weaker.[14] Another example occurred in 1954 when the U.S. orchestrated a covert action to overthrow the military government of Guatemala. Part of the covert operation entailed the broadcast of false, tactical field communications indicating that an army of thousands was invading

Guatemala from Honduras and El Salvador. In fact, there were only a few hundred Guatemalan exiles advancing on the Guatemalan capital. From their COMINT intercepts, the Guatemalan military government believed an entire army was advancing on the capital of Guatemala City, causing them to flee the state and resulting in a successful covert action.[15]

Cyber intelligence. Still not designated an official INT, cyber intelligence has taken on increasing importance in U.S. national security and law enforcement. Cyber intelligence entails collecting information from computer networks and information-processing systems. Publicly available cyber information accessible on the Internet (including social media) is considered part of OSINT (see below). Intercepting information transmitted over the Internet through emails and other digital communications (voice, facsimile, video, etc.) is considered COMINT. HUMINT covert collection usually is required when targeted computer networks are not connected to the Internet. Additionally, cyber warfare takes place when offensive information operations attack computer networks—meaning the cyber intruder may take control of or damage the network or associated industry. Cyber phases range from passive intelligence collection to offensive operations.

As of this writing, there is no single agency or office in charge of U.S. cyber programs. There is no "cyber czar" to coordinate aspects of U.S. government cyber activities. All government agencies and private sector entities have individual responsibility for protecting their own computer networks and information-processing systems through implementation of cyber security measures. With the vast majority of U.S. critical infrastructure owned by the private sector, DHS is responsible for coordinating voluntary cyber security guidance with the private sector and to collect cyber intelligence on threats to critical U.S. infrastructure. DHS also provides assistance to state and local governments to protect their online voting systems and other critical cyber networks. Military cyber intelligence collection is conducted and coordinated by NSA. Law enforcement cyber intelligence collection is focused on preventing or

investigating crimes and is conducted by individual law enforcement agencies, with the FBI having a major role in cyber intelligence coordination among law enforcement agencies at the federal, state, and local levels. U.S. military cyber warfare operations are under the purview of U.S. Cyber Command, which is collocated with NSA. Cyber intelligence is usually classified in two broad areas, known as computer network exploitation (CNE) and computer network attacks (CNAs).

Computer Network Exploitation (CNE). These activities are usually conducted against three different target types:[16]

Computers and intranets with Internet connection. An intranet is a computer network that is accessible only by authorized members and not accessible to the general public, even though it may be connected to the larger Internet. For example, a bank or other financial concern may have an intranet that is protected from entry by anyone without a proper login/password entry or secure virtual privacy network (VPN) protection. CNE conducted in this area targets servers, desktop and laptop computers, tablets, smart phones, or other devices (cameras, WIFIs, etc.) connected to a network through the Internet.

Intranets not connected to the Internet. The challenge here is to access the intranet from outside. Some networks will emanate electromagnetic signals, such as keyboard strokes or entire data streams from unshielded equipment, which can be collected if a covert HUMINT source can place sensitive technical collection equipment in range of the signals. Additionally, HUMINT sources may be able to develop a source who can access the intranet remotely or physically collect and provide information.

Stand-alone computers that do not connect to any network. Collection in this area also requires covert HUMINT sources to either obtain electro-magnetic signals from the stand-alone computer or physically access the computer to collect and provide information.

CNE includes a number of widely known techniques, including:[17]

- *Trojan horses,* which are "innocent" programs that conceal their true purpose to send information from the targeted computer network back to the collector. This could include logins, passwords, and data. With login information, the Trojan horse collector can enter the targeted computer network and extract data with no constraints.
- *Worms* are similar to Trojan horses, but are meant to remain concealed and undetected. Worms can be used to establish "backdoors" into the computer network for collecting data. Worms can even direct the transfer of money or data to unauthorized recipients.
- *Rootkits* often are concealed in a Trojan horse and are designed to allow the collector to take control of a computer network without being detected.
- *Keystroke loggers* are designed to capture and record computer keystrokes. Their main purpose is to capture logins, passwords, and encryption keys. Keystroke loggers may be implanted in the computer network's operating system or physically attached to a keyboard by HUMINT sources.

Computer Network Attacks (CNAs). These activities are supported by CNE and involve offensive information operations that are intended to degrade, disrupt, deny, or deceive a computer network or its owners. Examples include the

2005 Stuxnet worm attack on Iranian nuclear programs. The Stuxnet attack, perpetrators still unconfirmed, attacked Iranian supervisory control and data acquisition (SCADA) systems, degrading their nuclear weapons research and development activities. In 2015-2016, Russian military intelligence hackers conducted a cyber-attack on the U.S. Democratic National Committee (DNC) computer systems. The Russians stole embarrassing data from the DNC associated with the 2016 presidential election and released it to the public through WikiLeaks to disrupt U.S. presidential elections. In 2017, NSA-developed hacking software tools that were surreptitiously released to the public and have been used in a number of CNA attacks.[18] Box 5.2 describes a CNA-directed attack at U.S.-based Sony Pictures by the North Korean government.

Box 5.2 Computer Network Attack: 2014 Sony Pictures

In 2014, Sony Pictures was about to release the movie, "The Interview," a fictitious comedy about a plot to assassinate North Korean leader Kim Jung-un. The North Korean's warned Sony not to release the movie. In the face of North Korean threats, Sony chose to cancel the film's formal premiere and wide-scale theatrical release, and decided to go directly to a downloadable digital release and later limited-theatrical release. In response, North Korean government "hackers" began a CNA against Sony Pictures. They first spent several weeks accessing the network to learn how to do the most damage to the film studio. The hackers used a malware worm, which included a listening implant, backdoor, proxy tool (rootkit), destructive hard-drive tool, and destructive target-cleaning tool. They stole Sony network data to include emails and several pending movie releases, plus plans and scripts for future movies. The emails revealed embarrassing information on Sony actors, officials, and their families. The finished movie thefts significantly disrupted Sony's revenue stream for upcoming releases as North Korea made the movies available for free on the Internet. Additionally, the hack disabled and erased programs and data on 70%

of Sony's computer network. The North Korean attack cost Sony tens of millions of dollars and damaged relationships between actors and studio officials. This one case changed U.S. public perception of the capabilities and threats from computer network attacks.[19]

Cyber intelligence strengths and weaknesses. As with the official INTs, cyber intelligence has its strengths and weaknesses. Its primary strength is the large amounts of data CNE is capable of collecting; most importantly, the intentions of adversaries. Cyber intelligence weaknesses include its susceptibility to denial and deception. Denial includes the target's use of good cyber security measures to employ passwords, firewalls, encryption, VPN, and even lesser-known languages and dialects to protect their data. Disconnecting from the Internet is also a means of denial. As with COMINT, the target also may use misinformation; i.e., place false or altered data in its digital files to deceive the cyber intelligence collector. As the world becomes more reliant on computer networks, cyber intelligence will continue to grow in importance in national security and law enforcement analysis.

Imagery intelligence (IMINT). This includes the collection of optical (visual), infrared, and radar images of a target. It originally was labeled PHOTOINT. More recently, IMINT is referred to as **geospatial intelligence (GEOINT)**, which provides analyses combining imagery products with geographic information systems (digital mapping). U.S. employment of IMINT can be traced to the U.S. Civil War (1861-1865), when the Union Army employed hot-air balloons with daguerreotype photography to document Confederate Army troop dispositions. IMINT collection was expanded through use of aircraft in World Wars I and II, and collection by satellites began in the late-1950s and early-1960s. At first, satellite photographs were captured on film, and the film canisters parachuted to earth where they were recovered by specially equipped aircraft. By the 1970s, digital electro-optical devices were used to collect and transmit images directly to earth

stations. Today, imagery collection includes ground-based, fixed sensors, aerostats (unmanned tethered blimps), aircraft, unmanned aerial vehicles (UAVs, i.e., drones), and satellites. U.S. government IMINT is coordinated by the National Geospatial-Intelligence Agency (NGA), which is subordinate to the U.S. Department of Defense. NGA supports military operations, national security policy making, and earth resource management. NGA also oversees the Defense Mapping Agency, providing military and commercial paper and digital charts and maps worldwide. Commercial satellite imagery also is available to support an array of government and commercial activities. Google Earth is an example of commercial satellite imagery.

Selection of IMINT sensors depends on a number of factors. Some IMINT collectors can only provide a one-time "snapshot" of the target. This is mainly true for satellites and high-flying aircraft such as the U-2. Other IMINT collectors can provide continuous coverage of a target. This is true of ground-based sensors and aerostats, such as those deployed along international borders, or by low-flying aircraft, especially UAVs, that can remain on scene for long periods. Physics and weather are limiting factors in IMINT collection. Optical IMINT satellites are in sun-synchronous, low-earth orbits (200 to 1000 miles altitude); and the characteristics of their sensors limit the resolution of images. Sun-synchronous means the satellites are in polar orbits (pass near the north and south poles), making 24 orbits each day while passing overhead positions on earth within an hour or so of the sun's highest point of the day in that area. To obtain photographs more often than every 24 hours requires the launch of more than one IMINT satellite with orbits offset from when the sun is nearly directly overhead a position on earth. Optical IMINT collectors cannot see through clouds, fog, haze, heavy snow, or smoke; therefore, these collectors are not used during darkness, unless the targets are lights in a particular area or location. Infrared collectors also are impeded by clouds and are normally utilized at night when not competing with the sun's infrared interference. Radar imagery collectors are unimpeded by weather so they can be used around the clock.

IMINT strengths. IMINT provides flexible collection of information producing photographs or digital products that are very compelling to decision makers. By adjusting an optical camera's aperture and focal length, an IMINT collection platform can provide either imagery of a larger area or of a smaller, specific location. This flexibility comes at a cost to resolution. A wide-area optical image usually is obtained at lesser resolution (fewer image details). An image of a specific location may optimize the collection system's resolution and provide more details of a smaller area. One method to overcome the resolution problem with a wide-area image is to take a series of continuous, smaller-area images as the aircraft or satellite passes over a wider area.

The primary advantage of IMINT surrounds its ease of understanding by decision makers. People are comfortable with seeing and evaluating visual information as part of their everyday activities. When geographic location or movement is an analytic consideration, GEOINT allows the analysis and display of a combination of all-source information to include geographic locations on maps or charts, imagery of facilities, adversary dispositions, pipeline data, electrical systems, etc., or any other information that can be presented in a geographic format.

IMINT weaknesses and potential biases. In addition to being expensive, IMINT has a number of weaknesses that can lead to bias. First, remote imagery collectors cannot see activity or materials inside a building or underground facility. To look inside buildings and into underground facilities requires HUMINT collectors. Second, one-time, snapshot imagery does not show activities before or after the time of the image. Third, IMINT is susceptible to denial and deception, as when the target removes materials easily seen in an image such as placing aircraft in a closed hanger or under camouflage. The target also may present false information to deceive the target. For example, during preparations for the June 1944 Normandy landings, the Allies worked to convince the Germans the invasion

of France would take place near Calais, France. To deceive German collectors, the Allies deployed a limited number of reserve troops simulating pre-invasion activities (these troops would eventually be in second and third waves landed at Normandy). A deceptive COMINT plan mirroring landing force communications (see COMINT deception above) was deployed. They also created a deceptive force-presence scheme. The Allies built tent cities with no troop residents but with cooking fires blazing, inflatable mock-ups of artillery, tanks, and trucks—all placed in invasion-staging formations, and wood-framed and canvas-covered fake landing craft to help convince the Germans of preparations for the Calais invasion. German reconnaissance aircraft photographed the fake invasion force, resulting in the Germans diverting their attention from southwestern England where the real landing forces were actually being prepared.[20]

Measurement and signature intelligence (MASINT). These activities can be defined as, "…technically derived intelligence, excluding traditional imagery and signals intelligence, that when collected, processed, and analyzed, results in intelligence that locates, tracks, identifies, or describes the signatures (distinctive characteristics) of fixed or dynamic target sources."[21] In other words, MASINT includes technical intelligence collection not considered ELINT, COMINT, IMINT, or Cyber intelligence. It is mainly collected by a variety of military sensors and is used in military operations, defense acquisition and force modernization, arms control and treaty monitoring, WMD counter proliferation, counterterrorism, counternarcotics, and to support environmental intelligence gathering.[22] The U.S. Defense Intelligence Agency (DIA) has been the coordinator for MASINT since the discipline was instituted in 1986. Individual U.S. military services normally focus on the building and employment of the MASINT collection platforms related to their service missions.

The "M" in MASINT stands for "Measurement" and indicates the (usually indirect) measurement of collected information. The S, or "Signature," indicates the collection of distinct features or characteristics about the origin, source, and

functions of the collected information. MASINT may be used for strategic, operational, or tactical intelligence collection and/or to support military or law enforcement operations. MASINT includes a number of technical areas:

Electro-optical collection focuses on properties of emitted or reflected energy to include lasers and polarized or multi-spectral energy across the infrared, visible, and ultraviolet bands of the electromagnetic spectrum (i.e., outside of the normal visual and infrared collection of IMINT). For example, lasers are increasingly used for intelligence collection, weapons targeting, and as destructive weapon systems.

Geophysical collection is designed to detect anomalies in the normal physical properties of earth. Such anomalies may be seismic, acoustic, gravitational, or magnetic disturbances. For example, seismometers are used to detect nuclear weapon tests conducted in areas otherwise denied to collectors. Military antisubmarine warfare platforms use combinations of active and passive acoustic sensors (Sonar) and Magnetic Anomaly Detection (MAD) to locate, track, and attack submerged submarine targets, if necessary.

Materials collection supports analysis of the composition and identification of gases, liquids, and solids. MASINT or HUMINT collectors provide materials that undergo technical, chemical, biological, and radiological analysis. For example, because nuclear weapons production and testing can leave radioactive materials in the air or on the ground, HUMINT collectors can provide samples of the residue, which can then be analyzed by MASINT analysts in a military or national laboratory. Another example of material collection is law enforcement's use of handheld scanners to detect airborne and physical residue left behind by illegal methamphetamine production.

Radar collection focuses on short-range, line-of-site, synthetic aperture, and over-the-horizon radar systems (i.e., outside the normal collection of ELINT and IMINT). Battlefield short-range, line-of-site radars can detect detailed troop movements and assist targeting. Short-range, line-of-site radars may be sensitive enough to detect the firing location of incoming artillery shells. Synthetic aperture radars collect not only the location of a target but also provide the size and silhouette of the target. Over-the-horizon radar usually employs radio waves reflected off the ionosphere to obtain long-range detections. For example, over-the-horizon radars located in the United States have been used to detect drug-smuggling aircraft departing the north coast of South America and bound for the United States or nearby states.

Radio frequency collection focuses on wideband electromagnetic pulses, telemetry signals, and other non-communications signals in the electromagnetic spectrum (i.e., outside of normal collection of COMINT). Electromagnetic pulses are a byproduct of a nuclear explosion or can be used offensively through release of strong electric signal bursts that can disable electronic sensors, communications systems, and weapons. Cobra is a codename for a number of land-based, seaborne, and airborne MASINT collectors that focus on foreign intercontinental ballistic missile tests, including the collection of flight paths and telemetry signals from the test missile to its land controllers. After an unannounced foreign nuclear weapon test, airborne sensors can detect residual radiation emitted from the test site. Nuclear radiation samples look for the presence of electromagnetic gamma rays and x-rays.

MASINT strengths and weaknesses. The primary strength of MASINT is its ability to collect technical intelligence on targets outside normal ELINT, COMINT, and IMINT collection activities. MASINT information is critical to the U.S. military

in terms of both raw information collection and finished analysis on the production of weapons systems.

MASINT collection is expensive, not only in terms of the technical collection platforms required, but also in the employment of scientists to build the technical collection platforms and to analyze the raw information provided. Due to its highly technical nature, MASINT analyses may be unfamiliar to decision makers, who may not give results proper credence. Most MASINT collection is done remotely; but, when HUMINT support to MASINT is required, it can place the HUMINT collectors in dangerous situations. As discussed previously, HUMINT collectors must consider the "risk versus gain" in planning their collection activities.

Open-Source Information

Open-source information normally is available to all practitioners and academic analysts. Anything published for a public audience (books, magazines, movies, television, videos, newscasts, web sites, pod casts, etc.) is open-source information. This information is labeled **open-source intelligence (OSINT)** in security analysis circles. OSINT is organized and found in hundreds of individual, online commercial, and academic databases available to analysts. OSINT database subscriptions for the IC are coordinated through the ODNI. Small, local libraries to large university research libraries offer access to a significant number of OSINT databases. Some of these databases also may be available through the Internet. Analysts should keep in mind that not all of the world's knowledge is online. There will be occasions when the analyst must search in physical libraries, archives, public records, etc., to locate relevant open-source information. Most libraries, archives, and record centers have reference specialists to assist in finding specific information. Open-source information is critical to practitioners; approximately 85%-90% of the material in strategic analysis reports is drawn from open sources.

Searching OSINT sources. Each OSINT online database has a search engine, sometimes unique to the database. Most libraries, archives, and record centers have search engines to allow digital searching of their holdings in order to locate digitized and non-digitized materials; including paper holdings, microfilm, videos, etc., for the analyst to review. Some less-frequently updated open-source sites may require the physical searching of card catalogs and reference manuals to locate material. Most of the digital search engines use searches that employ keywords connected by Boolean logical operators "and," "or," and "not." For example, if searching a database for information on terrorism and Afghanistan, use of the limiting operator "and" (terrorism and Afghanistan) would return items including both terrorism and Afghanistan in the title or text. This is the most common type of search. Use of the inclusive operator "or" (terrorism or Afghanistan) would return a much larger list of items with either terrorism or Afghanistan in the title or text. Use of the excluding operator "not" (terrorism not Afghanistan) would return items with terrorism in the title or text but not those containing Afghanistan. Some databases have advanced search engines that allow the entry of several keywords and multiple Boolean operators to focus the search on specific items most appropriate for the analytic project's research question(s). Some search engines will access several databases simultaneously—always a plus in saving time. Analysts should be familiar with the many databases and their search engines that they will be expected to regularly access.

When searching OSINT databases, analysts must review each item returned to determine if the information applies to their specific research question(s). This may require the review of hundreds of potential sources to find the 40-60 actually used in an analytic project. The database searches should continue, time allowing, until there are either no new items found or when there is no new information being uncovered. Some items found may only require speed-reading (another skill valuable to analysts) or, if seemingly important to the analytic project, the item may require a more in-depth reading. Analysts must document the information found to include taking notes, making margin notations of using highlighters (but

not on original items), recording reference citations, and/or keeping paper or digital copies of relevant items. Recording full reference citations for all items uncovered is important as both practitioner and academic reports require proper documentation. Based on their agency and the analyst's own preferences, the analyst should establish a paper and/or digital filing system to organize and store information found in an open-source search.

Information searches differ based on the specific research question(s) being addressed. Some analytic projects may concentrate on individual agents or small groups, with a focus on the adversary's decision makers (agency analysis). Other research projects may concentrate on structural analyses. Chapters 3 and 7 provide additional discussion on agency versus structural analyses. In fact, most analytic projects will include a combination of both agency and structural analyses.[23] Agency analyses, also called leadership analyses, seek to uncover the points-of-views and assumptions influencing adversaries' decisions (Chapter 6). Information searches for agency analyses include uncovering what an agent has said, written, or done before on the specific or related research topic. It also is important to collect information on what others with access to the agent have said or written about the topic. Structural analyses look at the array of organizational, bureaucratic, legal, regulatory, and other structural factors influencing adversary decisions. When searching for structural information, it is recommended the analyst prepare a list of background and other structural information required by the analytic project to help focus the search effort. Figure 5.2 provides a sample list of background and structural information for researching terrorist groups.

Figure 5.2 Sample Background Information for a Terrorist Group Study

The group's origins, ideology, goals and objectives, public statements (verbal and written), organizational structure, leadership, funding or other sources of support, physical bases or operating/support location(s), recruiting methods, personnel strengths, training programs, communications methods, known

weapons/lethal agents and delivery methods, suspected weapons/lethal agents and delivery methods, past activities, standard operating procedures, propaganda programs, surveillance and intelligence capabilities and methods, and significant events/dates related to the movement.

When searching open source databases and reviewing items returned, there are three general categories of information to identify:

> *Facts* (data, evidence, information) that directly concern the analytic project. The analyst should try to confirm the facts uncovered by separate, independent sources. Facts may be found in raw reporting (such as in intelligence collection); in open sources, including statistical studies; and in information collected personally by the analyst.
>
> *Facts, combined with logic and reasoning*, which normally are found in statements of causality, arguments, and contentions (judgements, findings, conclusions, recommendations—Chapter 9), or theoretical propositions (axioms, theorems, postulates, laws—Chapter 3). Theoretical propositions are critical in creating models for conceptualizing the research project (Chapter 7). Statements, arguments, contentions, and propositions must be checked to ensure they do not include informal logic fallacies (Appendix I).
>
> *Logic and reasoning lacking facts* or statements or propositions that cannot be factually verified but employ logic and reasoning such that they may be classified as assumptions.

Prioritizing OSINT searches. OSINT sources vary in the reliability and validity of the information they provide. It is therefore recommended that sources be searched in order of their reputations for reliability and validity. Below is the recommended sequence for OSINT searching.

Governmental reporting. U.S. government agencies and international governmental organizations (IGOs) produce a number of recurring and special reports on a variety of subjects. IGOs are organizations or agencies where states are the members (United Nations, North Atlantic Treaty Organization, etc.). IGOs, such as the United Nations Office on Drugs and Crime, issue generally valid reports useful for national security and law enforcement projects. Most of these agencies and organizations employ professional researchers who can normally be trusted to provide objective and valid reporting. For example, U.S. Congressional Research Service (CRS) and U.S. Government Accountability Office (GAO) reports normally can be considered bipartisan and objective. There are a number of other U.S. agencies and IGOs that report on security topics under their purview. Analysts still should be wary of governmental reporting as at times it may slant toward supporting a particular government or IGO's program or ideology. Government reporting often is a good source of statistical data to support an analytic project.

Scholarly and professional articles. After government reporting, scholarly and professional articles are usually excellent sources of information. Scholarly articles are produced by academic researchers and published in academic journals. Most of the articles are refereed by panels of other academics (known as peer review). If not refereed, then the editors of the particular journal provide quality control on articles. Scholarly articles should be searched before scholarly books, as the scholarly publishing process usually first publishes the latest research results as journal articles before later including the material in books. Professional articles normally are published in journals or magazines. These articles usually are written by professional researchers or leaders in their professional field. For example, *National Geographic* and *Popular Mechanics* are good sources of professional articles. Analysts must assess the validity of scholarly articles, even if passing a refereed review, and of professional articles as they may

still lack validity. Scholarly articles often violate tenets of the scientific method and may not comply with proper sampling techniques (Chapter 3). Scholarly researchers may generalize results from a small or non-random sample to a population beyond what the sample supports. Figure 5.3 provides guidance for assessing categories of published material.

Figure 5.3 Classifying Scholarly/Professional Literature & Popular Media

	Scholarly, Professional Literature	Popular Media
Audience	Scholars, researchers, practitioners.	General public.
Authors	Experts in the field (i.e., faculty members, researchers, professionals). Articles are signed, often including author's credentials and affiliation.	Journalists or freelance writers. Articles may or may not be signed.
References	Includes a bibliography, references, footnotes, endnotes and/or works cited section.	Rarely include references or sources.
Editors	Editorial board of outside scholars (known as *peer review*), or professional editorial staff with subject expertise.	Editors and staff may not possess subject expertise.
Publishers	Often a scholarly or professional organization or academic press.	Commercial, for-profit publisher.
Writing Style	Assumes a level of knowledge in the field. Usually contains specialized language (jargon). Articles are often lengthy.	Easy to read – aimed at the layperson (written at 7th grade level). Articles are usually short and often entertain as they inform.
General Characteristics	Primarily print with few pictures. Tables, graphs, and diagrams are often included. Usually little if any advertising–if there is advertising, it is for books, journals, conferences, or services in the field. Often have "journal," "review," or "quarterly" as part of the title. Successive issues in a volume often have continuous pagination. Usually have a narrow subject focus.	Contain advertising and photographs. Often printed on glossy paper. Often sold at newsstands or bookstores. Usually restarts pagination with each issue. Usually have broad subject focus.

Scholarly and professional books. There are a myriad of scholarly and professional books. Scholarly books may be historical or scientific (including social science). Historical books provide details on a topic and are good sources for background information. Scientific books focus on presenting one or more theories and the facts, logic, and reasoning supporting the theories. Some books will be combinations of historical and scientific studies. Some scholarly books provide edited compilations of scholarly journal articles or chapters in the same subject area. For example, Editor Keith Logan's *Homeland Security and Intelligence* provides chapters written by several different authors covering aspects of homeland security intelligence activities.[24] Other scholarly books are an expansion of ideas in a previously published scholarly journal article. For example, Harvard Political Scientist Samuel Huntington took a journal article published in 1993 in *Foreign Affairs* magazine, "The Clash of Civilizations," and later expanded it into an entire book of the same title—one of the most discussed articles/books of the last few decades on world conflict.[25] Professional books usually provide detailed, descriptive material, lessons learned, and/or "how to" or other recommendations on a topic. Some books are hybrids that combine professional and scholarly material. For example, this book on using critical thinking in security analysis is considered a professional book as it covers the "how to" of security analysis; but, at the same time, is scholarly because it presents not only a theory of critical thinking but a number of supporting theories useful for security analysis.

Legal databases. Almost all national security, homeland security, and law enforcement analysis projects are embedded in a legal structure. Even if not lawyers, security analysts should understand and consider the legal structure applying to their particular research project. This is especially important in analytic security policy projects where the policy recommended must either comply with existing laws and regulations, or detail changes to laws and regulations. Legal databases have been developed to allow analysts to search

legal material, public records, and news reporting. Legal material also is available for legislation, statutes, treaties, regulations, court case transcripts, and associated case documents (briefs, pleadings, motions, settlements, and verdicts). Lastly, the databases include law reviews and law journal articles. Legal research assistants specialize in searching these legal databases. Westlaw and Lexis/Nexis are two competitors that organize and manage legal databases and allow access for a fee. Most law firms, libraries, businesses, and agencies, have subscriptions to either or both. Nexis is the news database material offered by Lexis/Nexis and provides popular media reporting discussed in more detail below.

Think tank and non-governmental organization (NGO) reporting. Dozens of academic and professional think tanks and thousands of NGOs produce research reports useful to analysts. Academic think tank reports normally do not undergo a refereed or peer review and, at most, are reviewed by local editors. Professional think tank and NGO reports also normally do not undergo a review beyond local editors. All think tank and NGO sources require extra scrutiny by analysts to ensure validity in the reporting as they are often rife with ideological slants that degrade validity. Think tanks often focus on a single issue or narrow set of issues. Some are supported by universities, others by contracts, grants, and donations from those interested in the think tank's issue areas and support its political orientation. Figure 5.4 provides a summary of selected think tanks and their political and ideological orientations that may be useful to security analysts.

Figure 5.4 Selected Think Tank Political Orientations[26]

Political Orientation	Think Tanks
Left/Liberal	Brookings Institution, Center for American Progress, Inter-American Dialogue, Human Rights Watch, American Civil Liberties Union
Centrist	Atlantic Council, Aspen Institute, Carnegie Endowment for International Peace, Center for Strategic and International Studies, Center of Immigration Studies, Council on Foreign Relations, Freedom House, Rand Corporation, Woodrow Wilson International Center for Scholars

Right/Conservative	American Enterprise Institute, CATO Institute, Claremont Institute, Heritage Foundation, Hoover Institution

NGOs include individuals or groups that organize around an issue area but do not represent federal, state, or local governments. There are hundreds of thousands of NGOs. A local book club or homeowner's association are considered NGOs. Of most interest to security analysts are NGOs that provide a combination of advocacy, research, and service in a security-related issue area. NGO political orientations often are highlighted by their title or by a quick review of their reporting or activities. Some NGOs, such as the American Civil Liberties Union, may be classified as both a think tank and an NGO, because it provides in-depth research, advocacy, and service (e.g., filing lawsuits) in the area of civil liberties. Analysts should assess the political orientation and validity of information accessed, whether from a think tank or NGO.

Popular media: newspapers, magazines, television, radio, blogs, and more. Popular media has a major advantage in collecting security information because reporters of larger media companies might be onsite and have observed world events firsthand. The major weaknesses of popular media are the sheer volume of information and that popular media often can suffer from severe validity problems. Figure 5.3 provides the general characteristics of popular media. The validity problem stems from material found in newspapers (including online news), magazines, television, radio, blogs, plus Internet-based social media. Validity issues begin with the popular media's political orientation and includes their approach to using factual data and the accuracy and depth of their analyses. Figure 5.5 provides a summary of the quality and political orientation of selected popular media. In general, centrist media sources of high- and medium-quality are the most useful to analysts. The low-quality media sources listed should be avoided or accessed with extreme caution. If accessed, high- and medium-quality sources with left/liberal or right/conservative political

orientations should undergo strict validity checks for bias. A particular problem with blogs and social media, of which there are thousands, is the presentation of **misinformation** and **disinformation**. Misinformation is false or inaccurate information, either mistakenly or deliberately disseminated. Disinformation is purposely communicated false information to mislead an audience (i.e., propaganda). As shown below, low-quality media sources, blogs, and social media sites frequently publish misinformation and disinformation to create inaccurate and unfair analyses. So, unless the blog or social media can be thoroughly evaluated for quality and political orientation, the information should not be used in security analysis.

Figure 5.5	**Selected Popular Media: Analysis Quality & Political Orientation[27]**
Political Orientation	**Media Sources**
	High Quality: Good Use of Facts, Advanced/Complex Analyses
Left/Liberal	*The Atlantic*, *Slate*, Vox, *The Guardian*, Axios
Centrist	*The Wall Street Journal* (news), AP, NPR (news), PBS, BBC, *Politico*, Bloomberg, Reuters, *USA Today*, *Time*, *Foreign Policy*
Right/Conservative	*The Wall Street Journal* (opinion), *The Economist*, The Hill
	Medium Quality: Good Use of Facts, Generally Fair Analyses
Left/Liberal	Local Newspapers (liberal cities/states), *The New Yorker*, *The New York Times* (opinion), MSNBC (opinion), CNN (opinion), *Mother Jones*, Huffington Post, *Vanity Fair*, BuzzFeed (news), *Slate*
Centrist	Local Television News, *The New York Times* (news), MSNBC (news), CNN (news), *The Washington Post*, NPR (opinion), Network News: ABC, CBS, NBC
Right/Conservative	Local Newspapers (conservative cities/states), Fox News/Business (non-political news), *The Washington Times*, *National Review*, *The Federalist*
	Low Quality: Poor Use/Made-Up Facts, Inaccurate/Unfair Analyses
Left/Liberal	Occupy Democrats, U.S. Uncut, Forward Progressives, David Wolfe, Palmer Report, Splinter
Centrist	*National Enquirer*
Right/Conservative	Fox News/Business (political news and opinion), Brietbart, InfoWars, Red State, One America News Network (OAN), *The New York Post*, *Newsmax*, Daily Caller

Internet sites. Because of often-severe validity problems with information posted on Internet sites, they are usually the last place a security analyst should search for information. Often government reporting, scholarly and professional articles/books, legal databases, think tank and NGO reporting, or popular media may be accessed on the Internet and could include the biases previously discussed. This warning on using Internet sites is for material beyond these sources, because anyone can set up an Internet site and post any written, voice, or video material they choose. In the United States, civil liberties conventions allow such unregulated publishing. There are some Internet sites considered in a "gray area," such as Wikipedia, because anyone can access it and change or update the site's articles to support their personal ideological slant. Thus, there is no real method for validity control on Wikipedia. The best a researcher can use this site for is to determine if the Wikipedia article coincides with other information found on a topic and then use the reference list included with most Wikipedia articles as sources to expand the information search on a topic. The analyst may find they must access the Internet, including the so-called "Dark Web," when researching terrorist or other threat groups to find their latest ideological or other statements—but be careful! The bottom line is to be suspect of all open sources until their validity is determined, which is especially true of Internet sites.

Circular reporting. While reviewing information from open sources, the analyst must be aware of potential circular reporting. This occurs when there often is only one unverified source for a piece of information, which then gets repeated through a number of open source and other reporting channels without other confirming evidence. Circular reporting is most noticeable in popular media and Internet reporting; but, at times, has been known to creep its way into government reporting and security analyses. "Echo chamber" is a term often used for when misinformation is amplified by circular reporting among popular media sources with ideological orientations. Box 5.3 describes a case of unverified

circular reporting that almost affected U.S. counterterrorism policy in Latin America.

Box 5.3 Circular Reporting: The Case of *al Qaeda* and MS-13[28]

After the September 11, 2001 (9/11) terrorist attacks on the United States by *al Qaeda*, there was increased emphasis in U.S. security and law enforcement communities to identify terrorist threats to the U.S. homeland. In looking south toward Latin America, officials found there were a number of state-specific insurgency groups—many reclassified as terrorist groups after 9/11—plus suspected linkages between Middle East terrorist groups with black-market activities in the Colombian La Guajira Peninsula and the Tri-Border region of Brazil, Argentina, and Paraguay. There were; however, no direct U.S. homeland terrorist threats initially uncovered in Latin America.

In early-2004, a report from Honduras indicated *al Qaeda* operative Adan G. El Shukrijumah was seen at an Internet-café in the Honduran capital of Tegucigalpa. Shukrijumah was a suspect in the 9/11 planning and a $5 million dollar reward was offered by the United States for his capture. It was speculated that Shukrijumah was meeting with the *Mara Salvatrucha* (MS-13) criminal gang in Honduras to enlist their support in smuggling *al Qaeda* operatives into the United States through the gang's established smuggling routes. MS-13 remains a violent, criminal gang. It expanded from its original bases in Los Angeles and El Salvador into Honduras, Guatemala, Mexico, and the greater United States, while also reportedly having cells in several other world states. MS-13 is deeply involved in the smuggling of humans, drugs, arms, and other contraband, in addition to being known for violent assaults and contract killings. Over time, due to its size and scope of criminal activities, MS-13 became a significant public security threat in Central America and Mexico.

The report of an *al Qaeda* and MS-13 meeting immediately caught the attention of the media and governments in Central America and the United States. Even without any confirming evidence, there was widespread media coverage about the meeting. U.S. media reporting raised anxieties over another potential *al*

Qaeda attack on the United States. Honduran Security Minister Oscar Alvarez raised alarms over the meeting, although it was believed he was using the report to help distract the Honduran public from his own repressive crackdown on gangs and to attract additional U.S. counterterrorism aid. U.S. Attorney General John Ashcroft also highlighted the reported meeting, in conjunction with a report that Shukrijumah had attempted to acquire radioactive material for the production and smuggling of a "dirty bomb" into the United States. (Shukrijumah was reportedly killed by the Pakistani military in 2014.)

The FBI and U.S. Department of Homeland Security investigated the report of *al Qaeda* meeting with MS-13 and determined there was no confirming evidence of such a meeting. The Guatemalan President and his Interior Secretary echoed the lack of evidence a meeting took place. Later, an academic researcher travelled to Tegucigalpa to inquire of government officials and journalists about the source of the original report. A Honduras-based journalist admitted he had made up the report.[29]

The consequences of this obvious case of false "circular reporting" easily could have affected U.S. security policy. It could have diverted U.S. attention and resources to an increased focus on counterterrorism in Central America, while also raising the status of MS-13 to that of a terrorist group—based only on one false report. This would have degraded U.S. security policy by wasting effort and resources on a non-existent terrorist threat.[30]

Analyst-Collected Information

Security analysts may find occasions when they must collect their own information. Personal collection of information is a major activity of academic researchers; but, if practitioner security analysts find they still have information gaps, they may have to collect their own. A complete discussion of analyst-collected information is beyond the scope of this book. It is recommended any analyst finding he/she must collect their own information consult with an

academic social science research methods textbook. Self-collected information activities are not easy and require significant planning and collection actions—all of which are covered in textbooks on research methods. Below is an explanation of several types of self-collection activities for consideration by analysts.

Interviews. Includes collection of information through interviews that may be *ad hoc*, semi-structured, or structured interviews. HUMINT collectors and qualitative academic researchers are trained in interviewing skills. First, the analyst (interviewer) must select the type of interview to conduct. *Ad hoc* interviews take place when the analyst has a chance (or quasi-planned) meeting with an interviewee (respondent) and has an opportunity to ask a few questions. The questions may not be prepared beforehand. *Ad hoc* interviews usually occur in a short time period, likely 10-15 minutes or less. Semi-structured interviews are usually scheduled for 30-60 minutes and employ a list of pre-planned questions prepared by the interviewer. As the semi-structured interview proceeds, the respondent is allowed to address other related topics, which normally also fill project information gaps. There are occasions where the semi-structured, pre-planned interview questions will not all be covered; for example, if the interviewer decides the related topics discussed have more value than some of the original questions. Structured interviews, usually of no more than 60 minutes, have a strict pre-planned list of questions. The interviewer attempts to keep the focus on the pre-planned questions and avoids straying to other topics. Respondents for all types of interviews are people the analyst thinks have the information needed. This could include senior government or military officials, academic specialists in the research topic, or even other analysts. Semi-structured and structured interviews are good for filling information gaps and confirming information found in other sources, but they take time to plan and execute. But, be careful, human respondents often provide the information they think the collector wants to hear or to use the collection process to bolster their own self-worth or other self-interests.

Focus groups. This type of collection is the equivalent of a group interview and generally consists of 8-15 people who are familiar with the research topic. It allows the analyst to obtain interview data from a number of respondents in a short time. Focus groups also provide unique information because they generate cross-respondent interactions that may provide different perspectives and often provide more information applicable to the analytic project beyond that from individual interviews. Focus groups originated in the World War II era, when groups of U.S. citizens were asked questions about war-rationing programs in order to tailor rationing marketing materials; and they still are widely used today in marketing and politics. For example, candidates in political campaigns often use focus groups to gain a sense of voter preferences. In academic research, focus groups are used to gather information and to validate interview and survey questions (see below). Most focus groups employ a moderator to ask the questions and keep the conversations flowing. Employing one or more note takers can also be useful. For accuracy in recording and analyzing focus group conversations, audio and video recordings of the focus group are recommended. Good focus groups usually last 45-60 minutes. The focus group collection also can be augmented with brief pre- and post-focus group surveys.

Participant-observation technique. When an analyst conducts participant-observation research, they go into the field and observe behaviors related to the analytic project. For example, if an analyst was working on a U.S. southwest border immigration project, he/she may plan a trip to personally observe the ongoing border activities. This could provide context and additional information for the project, including presenting opportunities for interviews or focus groups. If the analyst does not interact extensively with U.S. agency personnel or migrants, it is considered an indirect observation approach (see etic approach in Chapter 3). If the analyst interacts closely with U.S. personnel and migrants by joining their activities, then it is considered a direct observation approach (see emic approach in Chapter 3). HUMINT collectors and qualitative academic

researchers are trained in participant-observation techniques, but analysts may find a need for their own information collection using this method.

Unobtrusive measures. Similar to the work of forensic scientists in law enforcement cases, this type of information can be obtained from material people leave behind in their activities. For example, forensic scientists arrive after a criminal event to observe the scene and gather materials for analysis to assist case investigations. Security analysts may do the same; for example, after a terrorist attack or military battle, or during an inspection of seized, drug-smuggling vessels or aircraft. Unobtrusive-measures collection is not common in most security analysis projects, with the main exception being MASINT materials collection and analysis.

Content analysis. This type of analysis searches for specific information in written, audio, or video materials. This differs from COMINT content analysis and often is confused with larger literature searches. There are two types of content analyses defined here: quantitative (word count) and thematic.[31] Content analysis is especially helpful in agency leadership analyses to support points-of-view and assumption analyses (Chapter 6).

> ***Quantitative content analysis.*** These data collection efforts usually investigate a specific type communication or a single popular media source. It could be a newspaper, magazine, set of published speeches, etc., but the collection does not look at a broader literature. The analyst develops a list of concepts to be searched for and keywords corresponding to each concept. The compiled results (word counts) from a quantitative content analysis usually are subjected to descriptive or inferential statistical analysis. For example, as part of a terrorism study, the analyst may want to determine the personal characteristics of the terrorist leader. The analyst selects one source of data, possibly the leader's speeches over the past few

years, and develops concepts and words to indicate whether the leader's self-perception is one of being wise and/or powerful. Each instance of keywords and phrases found related to the concepts of wise and powerful would be recorded and then submitted for statistical analysis. This analysis also could provide insights into the terrorist leader's beliefs that could be useful in points-of-view and assumptions analyses (Chapter 6) in a larger analysis of the terrorist group's threat to the United States.

Thematic content analysis. In these data collection efforts, the analyst develops a short list of specific concepts or themes to search for in larger literature or a database. The analyst then reviews the literature and tabulates how many times the concepts appeared. For example, the analyst may want to research how a foreign terrorist leader evaluates the United States. This could be part of a research project to determine a foreign terrorist group's threat of attacking U.S. interests. The analyst then would look for evidence over the past few years of how many times in the terrorist leader's speeches, interviews, or COMINT intercepts, there was mention of the themes of U.S. policy toward the terrorist group or its supporters, U.S. capabilities to defend its interests, and U.S. successes against the terrorist group. Comments on U.S. policy might indicate if the group was friendly or hostile to the United States. Comments on U.S. capabilities could be measured on a continuum from weak to strong, and comments on U.S. successes could be assessed as either successful or unsuccessful. The compiled data from a thematic content analysis could then provide insights on points of view and assumptions as part of a larger analysis of the terrorist group's intentions to attack U.S. interests.[32]

Surveys. U.S. government agencies, IGOs, think tanks, NGOs, universities, and popular media inundate the U.S. populace with survey or polling data. These surveys possess varying degrees of validity. The key to evaluating survey validity is

to assess how the survey sample was taken (i.e., random or non-random), the size of the sample, and corresponding confidence level and confidence interval (see sampling theory in Chapter 3). Conducting surveys of large samples required to ensure validity of findings are costly in terms of time and money. Existing survey results should be reviewed by analysts if the survey focus supports their portfolio. For example, the NGO-conducted World Values Survey provides data on social, political, economic, religious, and cultural values of people in world states that is useful to analysts with regional or specific state portfolios.[33] The validity of survey results often are a concern, because respondents often provide answers they think the researcher wants, respond with outright misleading or false information, or purposefully try to deceive the researcher.

A survey-related procedure applicable to security analysis projects is the **Delphi Technique.** Created by the Rand Corporation in the 1950s, this technique calls for a survey of a limited number of respondents (10-15), usually not located in the same geographic area. Respondents, who are academic and/or practitioner specialists in the research topic, should not know the identities of other respondents. The technique calls for an initial survey to be sent to respondents with questions developed by the analyst. Based on data from all respondents on the same questions, the results of this survey are compiled and sent back to the respondents for re-evaluation of their original answers. In the second round of the survey, respondents will answer the same questions again, plus provide narrative comments of why they changed their previous responses or did not respond the second time with the majority of other respondents. The second survey results are then compiled, and both the responses and the narrative comments are returned to the respondents for a third round of answers and comments. The compilation of responses and narrative comments, and their return to respondents, are continued in additional rounds until the responses and narratives show little change. The goal of this technique is to allow the respondents to reach a consensus on the best views of the specialists, but still allow outlier responses that are explained by their respondents. The Delphi

Technique has been used with good success in security analysis.

Assessing Information

This chapter highlights the need for analysts to develop skills in information literacy and to become "critical consumers of information." As can be seen from previous discussions, there is potential bias in almost every type of information, whether obtained from intelligence collection, open sources, or even collected by the analysts themselves. This section provides three recommended analytic techniques to assist in assessing information. The first technique provides a template for analyzing sources. The second provides a checklist for detecting deception. The third provides a template for assessing the quality of information found in the information search.

Analyzing sources. Analysts should use a methodological approach for analyzing sources; Figure 5.6 provides a template for such analyses. This template follows the Security Analysis Critical-Thinking Framework. Using the template as a guide, analysts should take notes as they evaluate information found, including in lengthy intelligence finished reports; government, IGO, think tank, and NGO reports; and scholarly and professional articles/books. The template also can be modified to assess shorter works (raw intelligence reports, popular media, Internet material, etc.). Figure 5.6 includes notations to chapters and appendixes in this book with more detailed discussions of each checklist item. Results from analyzing sources should be used with the quality-of-information technique in Figure 5.8.

Figure 5.6 Template for Analyzing Sources

Source Full Citation:

1. The primary **purpose** of this material (chapter, article, book, video, etc.) is…… (Accurately state the author's purpose for this material. What was the author trying to accomplish? See Chapter 4.)
2. The key **question(s)** addressed in this material is/are…… (What key question(s) or problem(s) is/are addressed? See Chapter 4.)
3. The most important **information** in this material is…… (Identify the key information the author used to support their arguments/analysis. Identify the facts, data, evidence, experiences, statements, propositions, etc., that the author uses to reach their findings. See Chapter 5.)
4. The **context** of this material is…… (Identify the political, economic, social, historical, etc., background related to this material. This may include the existing knowledge on the subject as well as gaps in that knowledge. See Chapter 5.)
5. The main **point(s) of view** presented in this material is/are…… (Identify the author's views (perspectives, world views) of the topic. Points of view include beliefs and cultural factors, and can be theoretical, ideological, religious, methodological, etc., and usually play a large part in determining the main assumptions. See Chapter 6.)
6. The main **assumption(s)** underlying the reasoning in this material is/are……. (Identify the generalizations the author did not defend in the material. Assumptions are seldom specifically identified by authors. This is usually where the author's reasoning begins. See Chapter 6.)
7. The key **concept(s)** in this material is/are……. (Identify the most important definitions, ideas, models, theories, etc., used to support the author's reasoning. See Chapter 7.)

8. The **alternative(s)** considered in this material is/are…… (Identify any alternative answers to the key question(s) or alternative solutions or scenarios to the problem at issue that the author included in the reasoning. See Chapter 8.)
9. The main **inferences** and/or **interpretations** of this material are…….. (Identify the most important findings and conclusions the author presents in the material. What analytic methods were employed? Do the findings follow a logical argumentation approach? Are there any informal logic fallacies present? Are there underlying cognitive biases evident? See Chapter 9, Appendix I, and Appendix II.).
10. The main **implications** and **consequences** of this material are……..
    a. If this line of reasoning is accepted, the implications and consequences are…… (Identify the implications and consequences if the author's findings and conclusions are accepted. Identify those both the author states and those not stated. See Chapter 10.)
    b. If this line of reasoning is not accepted, the implications and consequences are…….. (Identify the implications and consequences likely to follow if people ignore the author's findings and conclusions. See Chapter 10.)

Deception detection. Almost all information is susceptible to deception, which can be defined as "[i]nformation…intended to manipulate the behavior of others by inducing them to accept a false or distorted perception of reality…."[34] Deception is as old as human conflict. Chinese General Sun Tzu (544-496 BCE) highlighted deception operations throughout his treatise *The Art of War.*[35] Operation Fortitude was the World War II Allies' highly successful plan to deceive the Germans on the exact location of their European invasion (discussed above under COMINT and IMINT).[36] Even when an adversary has a well-known history of deception, analysts may overlook it in their analytic judgments. When the stakes

are high, the analyst must consider the possibility of an adversary's use of deception. When the adversary has the capabilities to deny or manipulate the sources of key information, the deception detection review presented below should prove useful.

The possibility of deception should not be discounted even when there is no obvious evidence of deception. If deception is well done, the analyst should not expect to see any indicators of deception. The timing of the information and the *bona fides* of the sources might be a first indicator of deception.

Analysts should routinely check their information for deceptive efforts by an adversary. Figure 5.7 provides a checklist of questions to aid in detecting deception.

1. Does the adversary have the Motive, Opportunity and Means (MOM) to conduct deception efforts?
2. Would the potential deception be consistent with Past Opposition Practices (POP)?
3. Is there concern regarding the Manipulability of Sources (MOSES)?
4. What can be learned from the Evaluation of Evidence (EVE)?

Figure 5.7 Checklist for Deception Detection[37]

_____**MOM (Motive, Opportunity and Means)**
Motive (What are the deceiver's goals?)
Channels (What means for deception are available?)
Risks (What are the risks of discovery of the deception?)
Costs (Can the deception be accomplished?)
Feedback (Can the deceiver monitor the deception's effectiveness?)

_____**POP (Past Opposition Practices)**
Does the deceiver have a history of deception?
Does the deception fit past patterns?

Are there historical precedents?
Are there changed circumstances that would explain the deception?

_____**MOSES (Manipulability of Sources)**
Is the source reliable?
Does the source have access?
How good are the source's *bona fides*?
Is the source vulnerable to control or manipulation by the adversary?

_____**EVE (Evaluation of Evidence)**
How accurate is the source's reporting?
Is the whole chain of evidence available?
Does critical evidence check out?
Does evidence from one source conflict with others?
Do other sources of information corroborate the evidence?

Quality of information checks.38 Assessing the quality of information found is a key factor affecting the validity of any analysis. How much confidence an analyst places on their analytic judgments depends largely on the accuracy and quality of the information used in the study (Chapter 11). "Triangulation" of data sources, meaning using data from multiple sources to enhance the project's credibility, should be a goal of every analytic project. At times; however, use of multiple sources for data collection to check and recheck information is not possible. In any case, having multiple sources of information on an issue is not a substitute for having good information that has been thoroughly assessed. Examining the quality of the information used throughout a project helps the analyst avoid anchoring their analytic judgments on weak information.

Analysts must strive to understand the context and conditions under which critical information used in their research projects was collected and reported. Analysts should determine "what is known with some certainty" and "what is <u>not</u> known with some certainty," and continually assess motivations, ideologies, and

biases, plus check for inadvertent errors that may arise in the observation, interpretation, and reporting of the information.

Analysts should assess and annotate the quality of all information used in a project. A good first step is to use the Figure 5.8 checklist for assessing information. Ideally, analysts would develop databases where notes and annotations regarding the information's strengths and weaknesses can be entered for later searching and review by others. This may not always be possible, so analysts must assess the quality of all information (facts, data, evidence, etc.) that is used in their projects. To assess information, analysts should:

1. Systematically review all sources for accuracy (see Figure 5.6).
2. Identify information that appears the most critical or compelling.
3. Check for sufficient and strong corroboration of critical reporting. Try to triangulate sources and look for multiple sources with the same or similar evidence.
4. Consider whether ambiguous information has been interpreted and caveated properly.
5. Indicate a level of confidence (high, medium, or low) that can be placed on sources used in the project.[39]

Figure 5.8 is a template for recording information quality. Larger analytic efforts may uncover hundreds of items of information with facts, statements, propositions, and assumptions. It is not intended that all these items would be recorded in Figure 5.8. Instead, only record the most critical information to be further assessed and used to generate the analytic project findings. Figure 5.8 is intended to be used throughout the analytic project, adding new critical information as it is uncovered and assessed and deleting non-critical information as the analytic project progresses.

Figure 5.8 Template for Quality of Information Checks*				
Source	Critical Information	Corroboration of Information	Confidence Level (H, M, L)	Comments

* Add additional rows as needed.

Key Concepts

All-Source Intelligence
Analyst Collected Information
Case Officers
Circular Reporting (INTs)
Clandestine HUMINT Collection
Collection Disciplines
Communication Intelligence (COMINT)
Computer Network Attacks (CNA)
Computer Network Exploitation (CNE)
Content Analysis
Context
Covert Actions
Cyber Intelligence
Deception Detection
Delphi Technique
Disinformation
Electronic Intelligence (ELINT)
Electronic Support Measures (ESM)
Emission Control (EMCON)
Finished Intelligence
Focus Groups
Foreign Liaison
Geospatial Intelligence (GEOINT)
Human Intelligence (HUMINT)
Imagery Intelligence (IMINT)
Information
Information Literacy
Intelligence Collection
Interrogations
Interviews
Measurement and Signature Intelligence (MASINT)
Misinformation
Open Source Intelligence (OSINT)
Operational Analysis
Overt HUMINT Collection
Participant-Observation
Portfolio

Raw Information
Selection Bias
Signals Intelligence (SIGINT)
Signature Analysis
Strategic Analysis
Surveys
Tactical Analysis
Traffic Analysis
Unobtrusive Measures

Discussion Points

1. Using the completed Figure 4.4 Getting Started Checklist for a professional or academic analysis project (from Chapter 4 Discussion Points), outline a collection plan for your specific research question(s). Are there more potential sources than expected? What is the time frame for this information-collection effort?
2. Locate one source for your Question 1 professional or academic analysis project. Evaluate this one source using the Figure 5.6 Template for Analyzing Sources. What problems did you encounter in the evaluation? Would this be a good source for your analytic project?
3. Would your Question 1 (above) professional or academic analysis project require use of the Figure 5.7 Checklist for Deception Detection? Why or why not?
4. What advantages or disadvantages do you see with using the Figure 5.8 Template for Quality of Information Checks?

Notes

[1] Robert M. Clark, *Intelligence Collection* (Los Angeles, CA: Sage/CQ Press, 2014).

[2] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: WW. Norton & Company, 2004).

[3] Num 13:1-25 (Revised Standard Version).

[4] Jefferson Mack, *Running a Ring of Spies, Spycraft and Black Operations in the Real World of Espionage* (Boulder, CO: Paladin Press, 1996), 125-156.

[5] Jeffrey T. Richelson, *The US Intelligence Community* 5th ed. (Boulder, CO: Westview Press, 2008), 291.

[6] Department of the Army, *FM 2-22.3 Human Intelligence Collection Operations* (Washington DC: Department of the Army, 2006).

[7] U.S. Senate Intelligence Committee on Intelligence, "Study of the CIA's Detention and Interrogation Program (Washington, DC: U.S. Senate, December 2012). https://www.congress.gov/113/crpt/srpt288/CRPT-113srpt288.pdf (accessed December 23, 2021).

[8] Bob Drogin, *Curveball: Spies, Lies, and the Con Man Who Caused a War* (New York: Random House, 2007).

[9] U.S. National Intelligence Council, "National Intelligence Estimate: Iraq's Continuing Programs for Weapons of Mass Destruction" (Washington, DC: Central Intelligence Agency, October 2002).

[10] "Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction," March 2005. http://www.dtic.mil/dtic/tr/fulltext/u2/a441144.pdf (accessed June 25, 2018).

[11] Clark, 89.

[12] Ibid, 90.

[13] Ibid, 109.

[14] Lieutenant Colonel Michael J. Donovan, USMC, "Strategic Deception: Operation Fortitude" (strategic research project, U.S. Army War College, 2002), 11-12. https://apps.dtic.mil/dtic/tr/fulltext/u2/a404434.pdf#:~:text=OPERATION%20OVERLORD%2C%20a%20cross-channel%20invasion%20of%20Hitler%27s%20%22Fortress,British%20planners%20had%20been%20developing%20the%20deception%20plan (accessed October 20, 2020).

[15] Stephen Kinzer and Stephen Schlesinger, *Bitter Fruit: The Untold Story of the American Coup in Guatemala* (Garden City, NY: Doubleday & Company, 1982).

[16] Clark, 126.

[17] Ibid, 129.

[18] HBO, "The Perfect Weapon" (documentary, originally aired October 16, 2020).

[19] Ibid.

[20] Donovan, 10.

[21] Richelson, 245.

[22] Ibid, 245-246.

[23] Valerie M. Hudson, *Foreign Policy Analysis, Classic and Contemporary Theory* 2nd ed. (Lanham, MD: Rowman & Littlefield, 2014).

[24] Keith Gregory Logan, ed., *Homeland Security and Intelligence* 2nd ed. (Santa Barbara, CA: Praeger, 2018).

[25] Samuel Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Simon & Schuster, 1996).

[26] The Best Schools, "The 50 Most Influential Think Tanks in the United States," August 2020. https://thebestschools.org/features/most-influential-think-tanks/ (accessed October, 29, 2020).

[27] Table 5.3 compiled from a thematic content analysis of several Internet sources evaluating news bias. For additional information see https://mediabiasfactcheck.com

[28] Information for this case study is from a number of sources. In chronological order they included: *The Washington Times*, "*Al Qaeda* seeks tie to local gangs," September 28, 2004; *The Spokesman-Review*, "*Al Qaeda* recruiting in Honduras, officials says," October 31, 2004; Carlos Mauricio Pineda Cruz, "*Al Qaeda's* Unlikely Allies in Central America," The Jamestown Foundation, January 13, 2005; *Fox News*, "Feds Probe *Al Qaeda* Link to Latino Gang," January 14, 2005.

[29] Author was Research Director at the FIU Latin American and Caribbean Center, which sent the academic researcher to Honduras to investigate the reported *al Qaeda*-MS 13 meeting.

[30] Joseph Rogers, "Gangs and Terrorists in the Americas: An Unlikely Nexus," *Journal of Gang Research*, Vol. 14, No. 2 (2007).

[31] Hudson, 61-66.

[32] Example modified from a content analysis study by Ole Holsti of John Foster Dulles's view of the Soviet Union. Study summarized in Hudson, 62.

[33] World Values Survey. http://www.worldvaluessurvey.org/ (accessed November 1, 2020).

[34] Baron Whaley, "The Prevalence of Guile: Deception through Time and across Cultures and Disciplines," essay prepared for the Foreign Denial and Deception Committee, DNI, Washington DC, February 2, 2007, reprinted in Robert M. Clark ad William L. Mitchell, *Deception, Counterdeception and Counterintelligence* (Los Angeles, CA: Sage-CQ Press, 2019), 9.

[35] Sun Tzu, *The Art of War*, trans. Samuel B Griffith (London: Oxford University Press, 1963).

[36] Donovan.

[37] Sarah Beebe Miller and Randolph H. Pherson, *Cases in Intelligence Analysis, Structured Analytic Techniques in Action* (Los Angeles. CA: Sage-CQ Press, 2015), 75-77.

[38] U.S. Government, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," March 2009. https://www.cia.gov/library/center-for-the-study-of-

intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf (accessed November 4, 2020).

[39] Ibid.