Teams can take many forms. Ad hoc teams organized to deal with a specific issue probably are the most common. Teams are also created with an enduring mission and exist to support a specific set of customers. Fusion centers are used in the United States to support homeland security, law enforcement, and counternarcotics issues. The military services rely on joint intelligence centers to support deployed forces overseas.

Notes

1. R. V. Jones, "Scientific Intelligence," lecture to the Royal United Services Institution on February 19, 1947, *Journal of the Royal United Services Institute*, 92 (1947): 357.
2. Ibid.
3. "Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction," March 31, 2005, 19, 24.
4. Office of the Director of National Intelligence, "ODNI Mission and Vision," *ODNI's Weekly Intercept*, May 25, 2011.
5. "Report of the Commission on the Intelligence Capabilities of the United States," 416.
6. John H. Hovis, "CI at Avnet: A Bottom-Line Impact," *Competitive Intelligence Review*, 11 (third quarter 2000): 11.
7. Rob Johnson, *Analytic Culture in the U.S. Intelligence Community* (Washington, D.C.: Center for the Study of Intelligence, CIA, 2005), 76–79.
8. Martin Petersen, "The Challenge for the Political Analyst," http://www.csi.cia/studies/vol47no1/article05/html.
9. Walter Laqueur, *The Uses and Limits of Intelligence* (Piscataway, N.J.: Transaction, 1993), 53.
10. Gordon Negus, unpublished papers, 2007.
11. Hans Christian von Baeyer, *The Fermi Solution* (Portland, Ore.: Random House, 1993), 128.
12. Thomas Fingar, "Analysis in the U.S. Intelligence Community: Missions, Masters, and Methods," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, ed. Baruch Fischoff and Cherie Chauvin (Washington, D.C.: National Academies Press, 2011), 12.
13. Ibid., 20.
14. Ibid., 22.
15. Jonah Lehrer, "Groupthink," *The New Yorker*, January 30, 2012, 23.
16. Michael Herman, *Intelligence Power in Peace and War* (Cambridge, U.K.: Cambridge University Press, 1996), 275.
17. Quoted in Roger Z. George and James B. Bruce, *Analyzing Intelligence* (Washington, D.C.: Georgetown University Press, 2008), 167.
18. Johnson, *Analytic Culture in the U.S. Intelligence Community*, xiv–xv.
19. Douglas H. Dearth and R. Thomas Goodden, *Strategic Intelligence: Theory and Application*, 2nd ed. (Carlisle, Penn.: U.S. Army War College and Defense Intelligence Agency, 1995), 305.
20. John Rollins, "Fusion Centers: Issues and Options for Congress," CRS Report RL34070, January 18, 2008, http://www.fas.org/sgp/crs/intel/RL34070.pdf, 18–19.
21. U.S. Department of Justice, "Intelligence-Led Policing: The New Intelligence Architecture," NCJ 210681 (September 2005), 9.
22. Ibid.

19

A Network View: The Customer

Men will not look at things as they really are, but as they wish them to be.

Niccolò Machiavelli, *The Prince*

Some years ago, in a vignette that probably has been repeated many times, an elderly woman invested most of her savings in a Ponzi scheme—and of course, lost it all. When told of the loss, her investment advisor said, "Why didn't you talk to me first?" The woman's response: "Because I was afraid you'd try to talk me out of it!"

Policymakers are in a similar position. If they're contemplating a risky policy with no good choices, the last thing they need on the record is an intelligence analyst's conclusion that their choice is likely to fail. That typically makes them the most difficult customers to deal with. By contrast, policymakers respect and tend to listen to analysts who have spent the time needed to understand their policy concerns and have a demonstrated history of providing solid analytic products.

Along with policymakers, there are many other customers of intelligence analysis. Analysts should understand how the different types of customers operate and learn their perspectives on intelligence—the subject of this chapter.

Overview of Customers

This chapter focuses on the customers and purposes of analysis. It describes the intelligence requirements of various clients in government and the private sector, and the purposes and objectives that intelligence has in serving those clients.

The proper term, incidentally, is customers or clients—not consumers. Many people "consume" the intelligence that analysts produce. Only a few qualify as customers or clients, that is, persons whom the material is intended to serve.

Analysis is an addictive profession, in part because it poses frequent challenges and rewards. But it also can be frustrating, especially when after much hard work you have the answer to the intelligence problem and your

customer, for his or her own reasons, doesn't listen. Recall Sherman Kent's observation from chapter 1 that analysts have three wishes: "To know everything. To be believed. And to exercise a positive influence on policy." Let's look at each of these wishes in turn.

- The overall purpose of intelligence, as noted in chapter 2, is to *reduce uncertainty* in conflict. The key point here is that analysis doesn't deal with certainty. Both new analysts and customers find that at least disconcerting, even uncomfortable. Analysis can reduce but not eliminate uncertainty, and a key role of any intelligence manager is to help the customers understand that. Analysts may wish to know everything, but they are unlikely ever to reach that fortunate state. We just try to get as close as possible.
- Being believed depends on an analyst's credibility with customers. The fulfillment of this wish can depend on the analyst's reputation and the persuasiveness of the arguments to support his or her conclusions.
- Having an influence on policy (or, more broadly, on ensuing events) depends on the importance of the analyst's findings. As Michael Herman put it, "[A]uthority with governments is greatest where there is some connection with national security, and a need to cope with organized foreign concealment or deception."[1] Similarly, in a law enforcement or business context, the authority of the intelligence analyst is greatest when there is some connection with the organization's priority concerns, and a need to cope with an opposing (criminal or commercial) entity's concealment or deception. Stated another way: Just how much does the customer *perceive* that he needs your intelligence?

The numbers of customers of intelligence have expanded steadily over the past century from the traditional two groups—national and military leadership—to include a diverse customer set. In the United States, since 9/11, law enforcement and emergency response teams, for example, have become regular customers of intelligence. In many countries, such as China and France, commercial firms are major customers of government-provided commercial intelligence because of the competitive advantage that such intelligence gives them.

The SWOT methodology for strategic planning was introduced in chapter 2. In supporting SWOT planning, intelligence analysts identify opportunities and threats. Most customers have some idea of their internal strengths and weaknesses, albeit often a distorted idea. The uncertainty usually concerns the opportunities they have and the threats they face. From nonintelligence sources, customers often have some information on opportunities and threats—but this information varies greatly by customer. State Department policymakers and businesspeople often acquire very good information in the normal course of their jobs.

National-level customers and business leaders tend to focus on the threats in looking at intelligence, because of their pervasive fear of surprise. But intelligence serves best when it can provide notice of the opportunities.

Policymakers

The elite customers of national intelligence are generally referred to as policymakers. In the United States, this group is topped by the president. High on the list are the members and staffers of the NSC, which includes executives in the major cabinet departments. The premier current intelligence product for these customers is the president's daily brief (PDB). The national intelligence estimate (NIE) then is considered to be the primary strategic intelligence product. The NIE has been criticized over the years. An evaluation by Dick Kerr, a former deputy DCI, noted,

> The fundamental question is whether national intelligence estimates add value to the existing body of analytic work. Historically, with few exceptions, NIEs have not carried great weight in policy deliberations, although customers have often used them to promote their own agendas. The time may have come to reassess the value of NIEs and the process used to produce them.[2]

Several factors shape the way that policymakers view finished intelligence reports such as NIEs. Let's look at a few of them.

How Policymakers Differ

The policy culture is quite different from the intelligence culture, and many of the problems that arise stem from the difficulty of the two cultures in understanding each other. Policymakers, though, are a diverse group; and policymakers in the political, military, economic, and scientific and technical arenas are strikingly different in how they interact with analysts. The difference derives from the differing complexity of the problems that policymakers must deal with and their understanding of those problems. Policymakers tend to fall into these general categories:

- Policymakers in the political arena are traditionally the most difficult customers. They often understand politics better than the analysts do; most of them got where they are because of their political skills. They mostly possess good interpersonal skills; they believe that they read people well, independent of cultural background. And they have their own sources of information, independent of the intelligence community.
- Customers of scientific, technical, and weapons intelligence are likely not to be able to match the technical competence of the analyst in the analyst's special field. They usually need help in understanding the implications of intelligence and, accordingly, will give the analyst's opinions a substantial amount of respect.

- Policy customers of military and economic intelligence tend to fall in between these extremes. They have a good understanding of the subject matter but are more receptive to the intelligence analyst's assessments than policy customers in the political arena.

The Policymaker Environment

All policymakers work under severe time pressures in a disruptive environment. This work environment drives their preference for succinct messages. They need good analytic insights to help them deal with complex problems, often in a short time frame. Unfortunately, this is difficult to provide in the sort of in-depth study that characterizes strategic intelligence.

Former secretary of defense Robert McNamara described the policymaker's (and executive's) environment well. Looking back at his Vietnam mistakes, he observed, "One reason [we] failed to take an orderly, rational approach . . . was the staggering variety and complexity of the other issues we faced. Simply put, we faced a blizzard of problems, there were only 24 hours in a day, and we often did not have time to think straight. This predicament is not unique to the administration in which I served or to the United States. It has existed at all times and in most countries."[3] As a result,

- Policymakers have little time to make their needs known or to dialogue with the analyst.
- The intelligence message has to be clear, unequivocal, and usually brief—on one page, or even in the title of the article.
- Policymakers have short memories. They need to be reminded of past material—past knowledge cannot be assumed. They usually don't retain copies of prior intelligence.
- They have a "today's news" orientation; they tend to prefer current intelligence, and in-depth analysis often is less valued. Long-term research has to answer a question that the policymaker considers important.

The Policymaker's Mindset

A policymaker's job is, obviously, to make policy. Many of them come to their jobs with a preconceived idea of what the policy should be. Where they don't already have one, they frequently adopt a mindset, and after they have done so, the evidence must be overwhelming to change it. Their receptivity to intelligence typically changes over time. At the start of a new administration, intelligence analysts have their greatest impact. As policy views begin to harden, it takes more and more evidence to change anyone's mind.[4] Policymakers will demand more proof if the intelligence negatively affects their agenda, and they accept a much lower standard of proof when intelligence complements their agenda.

Many policymakers want to see the raw intelligence, often to select items to support their mindsets. National Security Adviser Zbigniew Brzezinski insisted on seeing raw intelligence, claiming that the intelligence community could not provide the broad, sweeping, bold insights into the future that he needed.[5] This policymaker or executive mindset has existed since there were leaders:

- In the sixteenth century, Philip II ruled the Spanish empire—the ultimate "hands-on" executive and typical of leaders before and since. He chose to accept incoming information from his far-flung intelligence network that supported his preconceived ideas and to avoid or ignore anything that contradicted them.[6] Like many executives since, Philip II was prone to wishful thinking.
- A CIA analyst in 1951 was studying the movements of the Chinese and had reached the conclusion that the Chinese had surreptitiously introduced their forces into North Korea. He briefed the assistant secretary of state for Far Eastern affairs, Dean Rusk, who later became secretary of state under Presidents John Kennedy and Lyndon Johnson. Rusk listened politely to the briefing, and at the end of it he said, "Young man, they wouldn't dare."[7] Weeks later, the Chinese attacked UN forces in Korea.
- Even directors of central intelligence have been trapped in mindsets. Former DCI Stansfield Turner believed that Ayatollah Khomeini was just another Iranian politician. Despite the arguments of his analysts, Turner briefed the NSC that after the overthrow of the shah of Iran, things would go on pretty much as they had before.[8]

An insidious problem with customer mindset is that the customer's subordinates (including both analysts and intermediaries) may be tempted to pander to it. It has been noted that Soviet intelligence—both the KGB and GRU—consistently told its leaders only what they wanted to hear.[9] During the Vietnam War, U.S. defense leadership did the same. Secretary of Defense Robert McNamara and the Joint Chiefs tightly controlled the flow of information to the president and had the ability to ensure that only favorable intelligence was shown to him. According to one presidential briefer, President Johnson "got very depressed and hard to handle when shown bad news."[10] In chapter 7, we examined the problems resulting from a flawed communications channel between collector and analyst. Worse problems are likely to occur when the channel between analyst and customer is corrupted.

Policymaker Priorities

National customers have an insatiable appetite for intelligence (though, as we'll discuss later, not necessarily for *strategic* intelligence). The U.S. intelligence community does not have the resources to satisfy all the demands of all its policy customers. So some sort of prioritization scheme has to be established.

In chapter 3, we noted that policymakers generally use informal channels to provide feedback about intelligence needs. But the United States does have a national-level prioritization scheme; in fact, it has had many of them. Several attempts have been made to formalize intelligence priorities since the National Security Act of 1947. The National Intelligence Priorities Framework (NIPF) is the current guidance from the DNI to the intelligence community on national intelligence priorities. It is reviewed by the NSC and approved by the president. The NIPF guides prioritization for the operation, planning, and programming of U.S. intelligence analysis and collection. The NIPF is updated semiannually. It takes the form of a matrix of countries and nonstate actors of intelligence interest versus a set of intelligence topics. It is used to guide both collection and analysis of intelligence.

Congress

Congress has become a major customer of U.S. intelligence—primarily, but not exclusively, as provided by the CIA. This role derives from Congress's responsibility to provide oversight of intelligence. Much focus of the oversight has been on collection and covert action, but analysis gets some attention.

Congress was not routinely given analytic products until the mid-1970s. From the very beginning, however, the CIA regarded Congress as an appropriate customer for its substantive analysis. Committees with a need to see such analysis might be permitted to read it, but for the most part, it was briefed to them by the DCI and other senior CIA officials. With the establishment of the Senate Select Committee on Intelligence in 1976 and the House Permanent Select Committee on Intelligence the following year, each with approved facilities for the storage of classified information, the main practical obstacle to sharing finished intelligence with Congress was removed.

More often, what provokes challenges and criticism is not what is briefed or delivered on the Hill. It is what members of Congress read in the newspapers indicating an apparent failure to predict an event that is important to U.S. interests. In chapter 17, we discussed the importance of not surprising the customer; that is true as well for Congress. Congress can handle almost anything but surprise. A study of Congress as a customer concluded, "Above all, the Agency [CIA] knew the chairmen of its subcommittees did not want to be surprised."[11]

The difficulty in having Congress as a customer for intelligence stems primarily from the tendency of individual senators and representatives to use intelligence as a weapon to affect policy that they don't like. Congress, though, usually isn't the source of leaks in the U.S. government. Leaks tend to come from administration officials who are trying to undermine policies with which they disagree. Congress can exercise its influence on policy via its budget authority.

When Congress asks a question, the intelligence community must respond and must do so on the congressional schedule. The result can be a disaster for intelligence, as noted by these authors in the case of the Iraqi WMD NIE:

> NIEs rarely represent new analysis or bring to bear more expertise than already exists in analytic offices; indeed, drafters of NIEs are usually the same analysts from whose work the NIE is drawn. Little independent knowledge or informed outside opinion is incorporated in estimative products. The preparation of an NIE therefore consists primarily of compiling judgments from previous products and debating points of disagreement. The Iraqi WMD estimate of October 2002 was characterized by all of these weaknesses and more. It was done under an unusually tight time constraint—three weeks—to meet a deadline for congressional debate. And it was the product of three separate drafters, each responsible for independent sections, drawing from a mixed bag of analytic product. Consistent application of analytic or evidentiary standards became next to impossible.[12]

Both policymakers and Congress often ask questions that are intended to get the answer that they want. This is the "Have you stopped beating your wife yet?" type of question. We introduced this type of question or, more generally, the poorly defined problem, in chapter 4 as the *framing effect*. Most policymakers and members of Congress are quite competent at applying the framing effect when posing questions, to get the answer that they want. Lawyers are experts at it. And, the mantra throughout this book is that if the question is poorly defined up front, the best subsequent analysis can't save it. Even if the customer did not deliberately frame the question, inexperienced analysts can frame it due to poor communication. A formal issue definition is needed to avoid it.

Business Leaders

Business customers of intelligence are similar to political policymakers, for many of the same reasons. They like to feel that they are in control and that they understand the competitive environment better than their business intelligence staff. They have mindsets. They face constant time pressures and are action oriented. But because they pay for their intelligence, they are more inclined to give specific guidance and pay attention to the analytic product. They are also more apt to take the analyst to task for poor outcomes.

The customers of business intelligence are highly varied in their interests and what they want from their intelligence units. In general, support to corporate strategy concerns issues such as acquisitions, identification of new markets or trends in existing markets, product development, and assessment of threats from competitors and criminal elements. Propensity to use intelligence varies by industry. The pharmaceutical industry, for example, has a tradition of relying on competitive intelligence.

As with national intelligence customers, business organizations have to prioritize their intelligence needs. A commonly used approach is one that was developed by the U.S. intelligence community during the early 1970s and subsequently abandoned. Competitive intelligence units, though, picked it up and adopted it. The technique is called key intelligence topics (KITs), which define intelligence priorities. From these are derived key intelligence questions (KIQs), which provide the questions that need to be answered to address the KITs.[13] The use of KITs/KIQs has thrived in the competitive intelligence world because it provides a structured approach to defining priorities and applying intelligence assets to those priorities, and because the resulting product has appeal for corporate executives.

Military Leadership

The U.S. military establishment has many customers for strategic intelligence, because many organizations within the Department of Defense, the Joint Chiefs of Staff, and the services conduct strategic planning. The secretary of defense might be considered the premier customer, and in the last decade, the Department of Defense has twice been headed by men who understand intelligence well: Robert Gates, a former DCI, and Leon Panetta, a former director of the CIA.

Military customers are usually clear about what they want from intelligence. Intelligence is an integral part of their world; they are used to seeing it and understand its value. Military leaders, like policymakers, vary greatly in articulating needs. All of them, to some degree, want to act as their own analysts—though policymakers are probably most inclined to do that.

The key problem that military intelligence organizations have is a tendency to overstate the strategic threat. Two factors that drive them in this direction are explained later in this chapter. Perhaps the earliest example recorded (in the Bible) occurred when the Israelites were spying out the land of Canaan. Their leader's objective (and mindset) was to conquer Canaan. His spies brought back unwelcome news, reporting, "[T]hey are stronger than we . . . there we saw the giants."[14] (This also was the earliest known example of intelligence's propensity to overstate a threat.) The Israelites wound up spending forty more years in the wilderness (there is no indication of what happened to the spies). Not surprisingly, there were no giants in the reports from the next set of spies, forty years later.

Military Operations

At the military operational and tactical levels, intelligence has a well-established role that is spelled out in military doctrine. Unit commanders are familiar with what intelligence can and cannot do. The relationship between intelligence and operations has been well settled by tradition. However, intelligence has become much more valuable to warfighters as it has gotten better. As noted in chapter 2, precision strikes require precise intelligence. The role of intelligence in warfighting has expanded steadily, and intelligence is a critical part of what is called a "revolution in military affairs."[15]

Homeland Security

The U.S. Department of Homeland Security (DHS) has been given broad responsibility for assessing both threats and risks to the U.S. homeland. In terms of the SWOT model, DHS therefore must assess weaknesses (risks) and threats. The major threats that the department focuses on are as follows:

- Domestic extremists
- International terrorists operating in the homeland or directing attacks against it
- Systemic threats such as pandemics and transnational criminal organizations

In fulfilling this role, DHS clearly is a customer for national intelligence organizations. But it also draws intelligence from state, local, and tribal officials and from the private sector.

Homeland Security is still evolving as a customer for strategic intelligence. Much of past DHS efforts have focused on the immediate threats to the homeland.[16] This appears to be changing as DHS matures and focuses more on the strategic view.

Homeland security intelligence at the tactical level typically involves providing intelligence from national collection assets to first responders. As an example, in the aftermath of Hurricane Katrina in 2005, Air Force U-2s and Air National Guard RC-26 aircraft flew photographic reconnaissance missions to support disaster relief. Since then, national-level assets have provided imagery and supporting analysis about wildfires (California, 2007) and oil spills (the 2010 Deepwater Horizon oil spill in the Gulf of Mexico).[17]

Law Enforcement

Law enforcement officials fall somewhere between policymakers and military operations customers in their use of intelligence. Some, such as counternarcotics teams, have experience in dealing with intelligence. Local police traditionally have limited experience with intelligence as it is done at the national level. Increasingly, however, as noted earlier, law enforcement groups rely on crime fusion centers (covered in chapter 18) to provide tactical intelligence, in particular; and acceptance of the value of intelligence analysis is increasing in the U.S. local law enforcement community. Fusion centers are similar in operation to the watch centers that intelligence agencies rely on. And cyber crime centers have been created in many states to bring together intelligence from national and local sources.

Up front, intelligence support to law enforcement must deal with a cultural challenge that shapes the nature of support across the strategic, operational, and tactical arenas. Intelligence in law enforcement, especially tactical intelligence, is intended to support specific investigations. It is tied

to action, usually in the form of making an arrest. The challenge has been stated as follows:

> Pure law enforcement focuses on building a legal case related to a crime that already has been committed—an historical perspective with a forensic cast. A case is carefully constructed based on admissible evidence. The evidence is handled in a prescribed manner. The rules associated with chain-of-custody are designed to protect the integrity of information and reduce the pollution of evidence as much as possible. A set of procedures is followed precisely to ensure the case will be successfully prosecuted. In comparison, intelligence agencies often collect information in a way that is not admissible in a U.S. Court. Law enforcement agencies are traditionally reluctant to use such information because of the potential of it being challenged and thereby jeopardizing a case.[18]

Some law enforcement organizations are moving from this investigative focus to a strategic focus. The emphasis on intelligence-led policing (discussed in chapter 2) has encouraged this trend. Much of this strategic intelligence deals with countering organized crime, specifically drug traffic and gangs. The strategy focuses on prevention and treatment as opposed to exclusively making arrests.

The security classification of intelligence creates difficulties for law enforcement. Raw reporting from HUMINT, IMINT, or COMINT sources is typically classified at the "Secret" level or higher, and local law enforcement officials typically have no security clearance. Conventionally this problem is handled by sharing information without source details—"I can't tell you why, but. . . ." Law enforcement officers are comfortable with that; they are used to taking unverified tips. Intelligence officers also frequently use fictional sources, often creating elaborate reports to conceal the true source and get the material released at a lower classification. But this is a balancing act; you can't protect sources and mislead analysts (who will evaluate a report depending on its source). Ideally, you use a fictional source that has the same general level of credibility as the real source.

What All Customers Want

We have pointed out repeatedly that the purpose of intelligence is to reduce uncertainty in conflict. Why is it so important? Because the effect of uncertainty on leaders and decision makers is profound across the entire spectrum of conflict. Uncertainty can result in the wrong decision, but its *effect* can be even worse than that. The problem starts with a natural tendency of executives to fear loss (or bad outcomes) in their decisions.

Most executives, including policymakers, military leaders, law enforcement commanders, and business executives, are guided in decision making by a principle known as *prospect theory*. Prospect theory says that people will pay a higher price, or risk more, to prevent losses than they will to seek gains.

Executives, especially in large bureaucracies, tend to be conservative and cautious. So they tend to believe intelligence that warns of losses, and to pay less attention to intelligence that suggests opportunities for gain.

This fear of loss, combined with uncertainty, can cause paralysis in decision makers. In 2006 a study by the economists Uri Gneezy, John List, and George Wu demonstrated a phenomenon that they called "the uncertainty effect." The basic idea is this: Expected utility theory says that people make risky decisions by balancing the value of all possible outcomes. Suppose that you're betting on the flip of a coin. If it's heads, you win $1.10. However, if it comes up tails, you lose $1. Overall, the expected utility of this gamble comes out in your favor—the potential payout is ten cents bigger than the potential loss, so you should accept the bet. But studies show that the vast majority of people won't accept this gamble. The possibility of a loss (and the associated uncertainty) outweighs the temptation of the extra dime. The Gneezy study cited specific examples of how the uncertainty effect leads people to make foolish decisions.[19]

This fear of loss (or for the decision maker, fear of a bad outcome), combined with the uncertainty effect, makes a deadly combination. We in the analysis business can't cure the fear of loss, but we can reduce uncertainty and thereby help the decision maker to make better decisions.

One opportunity for gain that will always catch the policymaker's or military leader's attention is the chance to deliver an asymmetric response. Although "asymmetric response" is currently a phrase having cachet, it is an old technique in conflict, both historical and allegorical. John Milton's epic poem, *Paradise Lost*, is premised on Satan's asymmetric response after his descent into hell. Instead of conducting another futile assault on heaven, Satan contaminates God's creation on Earth. Around 1600, the Dutch conducted asymmetric warfare against the Spanish in the Netherlands; they could move by water in the rivers more quickly than the Spaniards could, in some cases reaching in two days places the Spaniards could reach only in fifteen.[20] The Dutch built their successful conflict strategy around this advantage. The "Farewell" operation, discussed in chapter 8, was a superbly crafted asymmetric response to Soviet intelligence, and the intelligence officers supporting it received commendations. Intelligence that identifies opportunities for asymmetric response will always be welcome, so it is worthwhile to highlight the opponent's weaknesses and identify his vulnerabilities.

Analyst-Customer Interaction

All of the customer types described in the preceding section have mindsets. In the close interaction that is necessary to make the target-centric approach work, the pressures to conform analysis to policy usually are subtle. Intelligence that supports policy will readily be accepted and the analyst suitably rewarded; intelligence that contradicts policy encounters skepticism. This section discusses some ways of dealing with these pressures.

The traditional intelligence cycle diagram depicted in chapter 3 has a block labeled "dissemination" (see Figure 3-1). It's yet another indicator that the cycle doesn't really work that way. The report doesn't just go out the door and the analyst's job is done. Successful analysts know that the most brilliant piece of intelligence analysis may as well have gone into the trash if it is not read by the right people in time for them to act on it. Analysts using the target-centric approach make sure that the person who initiated the request sees their report or receives a briefing—ideally, both. They get copies to other people who may have an interest in the results. They ask for feedback from as many of them as possible. They can do these things because the customer has been involved in the process from the start.

As an analyst, you have to enter the interaction at the customer's level—which can be quite different when dealing with a president's national security adviser, a combat commander, a chief executive officer, or a police captain. The effectiveness of this interaction depends critically on the level of mutual trust and confidence between the customer and the analyst; and for policymakers the road to trust can be a long, hard one. A military commander and his intelligence officer can usually establish a high degree of mutual trust; they are working together for a common goal against a common enemy. Neither is much concerned that the other will share his confidences with the enemy. The policymaker and the analyst often have neither the common goal nor the common enemy. In Washington, D.C., the policymaker's enemy is often located just down Constitution Avenue, and she has to be aware that the intelligence officer might defect to that enemy at any time. For their part, analysts constantly have to be aware that their assessments may be twisted or misconstrued to fit a policy preference.

Assuming that some level of trust can be established, the analyst next has to do two things: get the customer to understand the message, and get buy-in, that is, get the customer to accept the message and act on it, even if the message runs contrary to the customer's mindset.

Analyst as Communicator: Getting the Customer to Understand the Message

A major problem of intelligence in sixteenth-century Europe was that spies could readily acquire the information, but governments could not readily grasp its significance and act accordingly.[21] Issues are much more complex today, but the challenge for analysts is still to help customers grasp the significance of intelligence.

Effective analysts must learn the skills of effective communication, in both writing and speaking. There are procedures for writing a report or presenting a briefing, some generally recognized across professions and some that are institution specific. Analysts learn their particular intelligence organization's technical quality and style guidelines and then pay strict attention to them. Analysts who develop communication skills must follow the conventional standards for

publications in their area and use terminology that their customers understand. In general, they should address problems and issues that interest customers and present results that

- Are forward looking, with detailed predictions of future developments or of major trends in the subject area and descriptions of the factors driving those trends
- Contain clearly stated conclusions supported by in-depth research and technical reasoning
- Include clear tutorials or explanations of complex technical subjects aimed at the expected customer

Moreover, analysts have to do all this *succinctly*, as discussed later in this chapter.

One cause of intelligence failure is what has been referred to as the "pathology of communication." That is, it is often hard to get the customer to believe intelligence judgments where policy issues are concerned.[22] Furthermore, analysts must convey areas of uncertainty and acknowledge gaps in their knowledge. The Iraqi WMD Commission noted, "Analysts also have a responsibility to tell customers about important disagreements within the Intelligence Community. . . . In addition to conveying disagreements, analysts must find ways to explain to policymakers degrees of uncertainty in their work."[23] To do these things without causing the customer to totally disregard the intelligence is a challenge.

The answer to both of these problems lies in the target-centric process. You have to make the customer a part of the intelligence process—which is difficult in the case of the busy policymaker. But once the customer is engaged in the process, communicating the results becomes much less difficult, and the customer is much more likely to understand and use the intelligence. The British model, discussed in chapter 18, has demonstrated that this approach works.

Finally, in preparing intelligence on technical subjects, there is always an easier way, always a clearer way, always a more accurate way to say something. Unfortunately, they are not the same way. It is almost axiomatic that if a scientific and technical intelligence report is readable and understandable, it is technically inaccurate. Only a highly skilled analyst can achieve technical accuracy and readability in one document. The answer? Don't place consuming emphasis on technical accuracy at the cost of readability. It is far more important to have the message understood and acted upon.

This demand for precision of expression is obvious in scientific and technical intelligence, but it occurs across all disciplines in intelligence, and for a good reason. Intelligence analysts often find that their words are interpreted (or misinterpreted) by policy customers to fit with the customers' preferred course of action. The response by analysts, especially in NIEs, is to make precise

expression an art form that is studied and practiced. As Michael Herman noted, precision of expression is rated very highly by analysts and their managers in intelligence communities in both Britain and the United States.[24]

Analyst as Advocate: Getting Buy-In

If analysis is conducted as it has been promoted in this book, the customer will usually accept and make use of the analysis results. But if the customer does not give a positive response, the analyst must shift his or her interpersonal skills in the direction of advocacy and act as a spokesperson in support of the conclusions.

Determining requirements and needs is marketing—finding out what the customer wants. This section is about sales—getting the customer to want (and use) what you have. The proper analytic attitude is made clear throughout this text: one of objectivity. But once analysis is finished, political realities set in. Analysts must sell the product because they quickly encounter one of the fundamental principles of physics that is also a fundamental principle in intelligence (see Analysis Principle 13-2): Every action produces an equal and opposite reaction. Analysts are often tasked because there is disagreement about an issue. It follows that their results, then, will be met with skepticism or outright opposition by some.

Recognize, however, that "selling" is a controversial recommendation. The Iraqi WMD Commission report criticized this tendency, noting, "In ways both subtle and not so subtle, the daily reports seemed to be 'selling' intelligence—in order to keep its customers, or at least the First Customer, interested."[25]

Analysts nevertheless often have no choice but to advocate for the product. Ideally, intelligence would be a commodity like food—consumers buy it because they need it. In operations, especially in military operations, that tends to be the case. Unfortunately, in policy support, it is more like insurance: It has to be sold, and buyers have to be convinced that they are getting a good product. Former secretary of state Henry Kissinger, on being reminded by an analyst that he had been warned about the impending outbreak of a war, reportedly said: "You warned me, but you didn't convince me."[26] The implication could not be clearer. If policymakers expect intelligence analysts to convince them, analysts have to persuade. There is a caveat: It can be very tempting to tell the customer what he wants to hear, simply because of the customer's professional position or power, and analysts should guard against it.

One problem of looking at intelligence as sales, especially in policy matters, is that it increases the danger of telling customers what they want to hear.[27] Another challenge is that the analyst needs a good sense of timing (as every salesperson knows).[28] Nevertheless, veterans of the analysis business have consistently noted the need to conduct a sales job. As Martin Petersen, author and former CIA senior intelligence officer, observed, "The reality for intelligence officers is that we must woo them [policymakers], sell them on the need for our services, and demonstrate the value of our material daily through its timeliness and its sophistication."[29]

If the customer is a U.S. government policymaker, the analyst typically must interact with lawyers, a relationship that is much different from what analysts are accustomed to and one in which advocacy skills are useful. Lawyers prefer to use intelligence experts as they would use scientific experts in a courtroom: receiving testimony on the facts and opinions, cross-examining, determining the key issues, and deciding. The existence of a controversy and of differing opinions is essential, in the attorney's view, to establishing the truth. Lawyers are uncomfortable with a single expert opinion and with the intelligence compartmentation system. To them, the intelligence community's traditional compartmentation system for protecting sources and methods is suspect because it tends to conceal evidence and is therefore inconsistent with the goal of the discovery process in civil litigation.

Many intelligence analysts have difficulty being advocates because it goes against their objective nature. The advocacy process is an adversarial one, and the guidelines for conduct come from the legal profession, where advocacy has been raised to a fine art and where the pitfalls of improper advocacy are well understood. R. V. Jones once observed, "When an analyst participates in an adversary process he is, and should conduct himself as, and should expect to be treated as, an advocate. The rules for an adversary process are different from those of research. The former permit biased or slanted testimony and the latter are directed toward objective evaluation."[30] Jones did, however, reserve judgment as to whether the giving of "biased or slanted testimony" was compatible with honor in a scientist.[31] Most analysts would undoubtedly argue that slanting the intelligence product is unethical and is always a bad idea, even if the customer consequently makes a bad decision.

Furthermore, obtaining acceptance from any customer can often depend on the analyst's reputation. A reputation for credibility and veracity among customers is the analyst's most valuable asset. It takes a long time to build and can be lost in a day. Or, as David Landes observed, "In the public domain, a reputation for veracity is worth more than valor and intelligence, and this especially in a world of ubiquitous guile and duplicity."[32] You need to get the customer to pay attention, but you cannot sacrifice credibility or truth to do it. If you do, you might as well get out of the business. A few examples:

- The KGB was discredited in the eyes of Soviet leadership when the Farewell operation became public, and all of its materiel acquisition results were called into question.
- During the Vietnam War, the CIA discounted and underestimated the magnitude and significance of North Vietnamese support reaching the Viet Cong through Cambodia's port of Sihanoukville. Subsequent information from a newly recruited source in the Cambodian port showed

that the agency's estimates were wrong and the military's were more accurate. Afterward, whenever the CIA disagreed with the Pentagon, the White House would ask DCI Richard Helms: "What about Sihanoukville?"[33]

- The Iraqi WMD miscall damaged the credibility of several intelligence community analysis groups, especially the CIA's. It will take years to overcome that damage.

We've discussed the issues that occur when the customer must deal with uncertainty. The greatest challenge that an analyst faces, though, is when the customer is certain—and wrong. This is the "false or flawed model" problem, and it is pernicious because it is almost impossible for any amount of intelligence to eradicate the flawed or false model. Former NIO Paul Pillar described the cost of policymakers' false models in his book *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform*. Policymakers began with a mindset (a mental model) of the Mideast situation and the Saddam Hussein–Al Qaeda relationship that was wrong. They subsequently selected the fragmentary evidence that supported the flawed model (known as cherry-picking) and ignored more substantial evidence to the contrary.[34]

The Unique Defense Analysis Challenge

The intelligence analyst in a defense organization must deal with two distinctive challenges: the premium placed on warning, and the pressure to produce threat assessments that align with policy.

The Premium Placed on Warning

Defense analysts have a special obligation to give their leaders warning of hostile military actions. The failure to warn has more severe consequences than does excessive warning. As Michael Herman observed: "Underestimation is less readily forgiven than overestimation."[35] And "it is more satisfying, safer professionally, and easier to live with oneself and one's colleagues as a military hawk than as a wimp."[36]

This pressure and resulting tendency of defense analysts to overestimate a threat is well documented and policymakers compensate for it—which leads to the desensitization issue discussed in chapter 16.[37] The result, though, is that the credibility of the defense analyst suffers.

Threat Assessments That Support Funding or Policy Decisions

Herman also observed that "[t]hreat assessments have always been one of the military cards in bargaining with treasuries."[38] The Backfire bomber case of chapter 9 and the URDF-3 (particle beam weapon) case of chapter 11 are examples of such threat assessments as bargaining tools. The tendency is to overstate the threat to justify funding or to support defense policy positions. The resulting concern, as Herman noted, is that U.S. defense intelligence organizations "have always had fairly low esteem."[39]

Defense analysts have to break away from the trap of aligning assessments with funding or policy decisions by providing objective analysis even when it runs contrary to the official position of their service or of the defense establishment. It would be disingenuous, however, to say that those who have done so have always fared well. Gordon Negus, former executive director of the DIA, told of how Major General Lincoln Faurer, while director of the DIA, dealt with pressure to conform intelligence analysis to funding. When Jimmy Carter was president, the White House was considering options for dealing with the Soviet Union's improved air defense system. Two of the options were to build the B-1 bomber or to arm the existing B-52 fleet with cruise missiles. The U.S. Air Force wanted the B-1. But the DIA's intelligence indicated that the Soviets felt much more threatened by the cruise missile option, which would nullify the Soviet Union's massive air defense investment. The Air Force chief of staff told Faurer, in unequivocal terms, to revise the DIA estimate to support the Air Force position. Faurer refused and was gone from the DIA within a month.[40]

Although the pressure to conform estimates to funding or policy is especially severe in the military, it is not unique to defense. Any analytic group that is closely connected to a policy group has to deal with this problem. As noted in the introduction in chapter 1, the British Foreign and Commonwealth Office forced the intelligence process to its desired conclusion that Argentina would not attack the Falklands in 1982. Departmental intelligence units such as the State Department's Bureau of Intelligence and Research, for example, face pressure to make intelligence fit policy. The State Department has long recognized this potential problem and attempts to keep its analysts separate and organizationally shielded from the pressures of policymakers.

Appropriators also recognize this tendency, and they usually follow the rule for using an organization's test results, discussed in chapter 7. That is, if the reporting organization has a stake in what an intelligence report says, and if the report supports the organization's position or interests, the appropriator will typically view the conclusions with suspicion.

Summary

Intelligence customers vary greatly in their willingness and ability to express their needs and to make use of intelligence. Policymakers are probably the most difficult customers, because of their pressure-cooker work environment and their tendency to adopt a mindset. Customers of political intelligence are the least receptive of the group; weapons systems and scientific and technical intelligence customers are the most receptive. Military, economic, and business customers typically fall somewhere in between.

Military leaders and military operations customers understand and value intelligence. Intelligence has a well-established role, and it is becoming more important especially at the tactical unit level. Law enforcement officials also increasingly understand the value of intelligence and how to use it; their problem is that they don't usually have the clearances needed to deal with classified

material. Business leaders vary in their use of intelligence, depending on the industry and their own background; but because they pay for the intelligence, they are generally inclined to make use of it.

In dealing with these customers, analysts have two challenges: to get the customer, first, to understand the message and, second, to accept and make use of the analytic results. Making intelligence understandable requires communication skills and empathy—the ability to put yourself in the place of the customer. Getting the customer to accept and make use of intelligence may require that the analyst become an advocate—a controversial and risky step. Acceptance also depends on the customer's view of the analyst's reputation.

All customers rely on intelligence to reduce uncertainty; when the level of uncertainty is high enough, customers will avoid making any decisions. As explained by prospect theory, customers tend to be more willing to accept intelligence about risks of loss or bad outcomes and less willing to make use of intelligence about opportunities for gain.

Threat assessments that support an intelligence organization's funding or policies (or those of its parent department) are usually received with skepticism—and should be. The tendency to shape analysis to support funding has been a special problem for defense intelligence organizations and often damages their credibility.

Notes

1. Michael Herman, *Intelligence Power in Peace and War* (Cambridge, U.K.: Cambridge University Press, 1996), 380.
2. Richard Kerr, Thomas Wolfe, Rebecca Donegan, and Aris Pappas, "Collection and Analysis on Iraq," *Studies in Intelligence*, 49, no. 3 (2007), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Collection_Analysis_Iraq_5.htm.
3. R. McNamara, with B. VanDeMark, *In Retrospect: The Tragedy and Lessons of Vietnam* (New York: Vintage, 1966), xxi.
4. CIA Center for the Study of Intelligence, "Watching the Bear: Essays on CIA's Analysis of the Soviet Union," Conference, Princeton University, March 2001, http://www.cia.gov/cis/books/watchingthebear/article08.html, 18.
5. Ibid., 19.
6. Geoffrey Parker, *The Grand Strategy of Philip II* (New Haven, Conn.: Yale University Press, 1998), 74.
7. CIA Center for the Study of Intelligence, "Watching the Bear," 14.
8. Ibid., 18.
9. Dino Brugioni, *Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis* (New York: Random House, 1990), 147.
10. Ibid., 573.
11. Britt Snider, *The Agency and the Hill: CIA's Relationship with Congress, 1946–2004* (Washington, D.C.: CIA Center for the Study of Intelligence, 2008), 10.
12. Kerr, Wolfe, Donegan, and Pappas, "Collection and Analysis on Iraq."
13. Jan P. Herring, "KITs Revisited: Their Use and Problems," *scip.insight*, 5, no. 7 (July 2013), http://www.growthconsulting.frost.com/web/images.nsf/0/CA6928E7B5561B6086257BB000452B41/$File/SCIP13V5I7_BFTP.htm.
14. Bible, Numbers 13: 31–33.
15. Anthony D. McIvor, ed., *Rethinking the Principles of War* (Annapolis, Md.: Naval Institute Press, 2005), part 5.
16. Mark A. Randol, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress* (Washington, D.C.: Congressional Research Service, March 19, 2010).
17. Maj. Mirielle M. Petitjean, "Intelligence Support to Disaster Relief and Humanitarian Assistance," *The Intelligencer*, AFIO (Winter/Spring 2013), http://www.afio.com/publications/Petitjean_ISR_Spt_to_HA_DR_WinterSpring2013_AFIOIntelligencer.pdf.
18. AFCEA Intelligence Committee, *The Need to Share: The U.S. Intelligence Community and Law Enforcement* (Fairfax, Va.: Author, April 2007), 5.
19. Jonah Lehrer, "The Uncertainty Effect," *Wired*, December 6, 2010, http://www.wired.com/wiredscience/2010/12/the-uncertainty-effect/.
20. Parker, *The Grand Strategy of Philip II*, 284.
21. Ibid., 213.
22. Douglas H. Dearth and R. Thomas Goodden, *Strategic Intelligence: Theory and Application*, 2nd ed. (Carlisle, Penn.: U.S. Army War College and Defense Intelligence Agency, 1995), 197.
23. "Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction," March 31, 2005, 419.
24. Herman, *Intelligence Power in Peace and War*, 105.
25. "Report of the Commission on the Intelligence Capabilities of the United States," 14.
26. Roger Z. George and James B. Bruce, *Analyzing Intelligence* (Washington, D.C.: Georgetown University Press, 2008), 80, 113.
27. Dearth and Goodden, *Strategic Intelligence*, 153.
28. Ibid., 156.
29. Martin Petersen, "What I Learned in 40 Years of Doing Intelligence Analysis for US Foreign Policymakers," *Studies in Intelligence*, 55, no. 1 (March 2011).
30. "The Obligations of Scientists as Counsellors: Guidelines for the Practice of Operations Research," *Minerva* X (January 1972): 115.
31. R. V. Jones, "Temptations and Risks of the Scientific Adviser," *Minerva* X (July 1972): 441.
32. David S. Landes, *The Wealth and Poverty of Nations* (New York: Norton, 1998), 167.
33. David S. Robarge, "Richard Helms: The Intelligence Professional Personified," *Studies in Intelligence*, 46, no. 4 (2007): 35–43.
34. Paul R. Pillar, *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform* (New York: Columbia University Press, 2011).
35. Herman, *Intelligence Power in Peace and War*, 247.
36. Ibid.
37. George and Bruce, *Analyzing Intelligence*, 80, 113.
38. Herman, *Intelligence Power in Peace and War*, 248.
39. Ibid., 240.
40. Gordon Negus, unpublished papers (2007).