# 3

# The Intelligence Process

*The power of accurate observation is commonly called cynicism by those who have not got it.*

George Bernard Shaw

George Lucas's original *Star Wars* movie describes the final stages of a human intelligence operation. The heroine, Princess Leia, places the plans for the evil Galactic Empire's ultimate battle machine, the Death Star, into the robot R2-D2, which is functioning as a mobile dead drop.[1] R2-D2 gets the plans to the rebel forces, whose scientific intelligence analyst briefs the rebel command on the plans, pinpoints the weak spot on the Death Star, and presents a brilliant analysis of the enemy defenses. Rebel fighter jockeys deliver proton torpedoes to the weak spot and destroy the Death Star. End of movie.

This *Star Wars* vignette accurately summarizes the intelligence process as it is popularly viewed. The people who collect intelligence information and execute the operations get the glory, the press, and the money. The intelligence analyst, working behind the scenes, gets the interesting problems to solve to make it all work.

Although the popular focus is on collection, most of the major failures in intelligence are due to inadequate or nonexistent analysis, and most of the rest are due to failure to act on the analysis, as noted in chapter 1. The information is usually there, at least in hindsight. So, unfortunately, is a large volume of misleading or irrelevant material that has to be examined and discarded. All intelligence organizations today are saturated with incoming information. Furthermore, in large intelligence communities, critical information about an intelligence matter may not be shared effectively because the intelligence activity is organized around the flawed concept of an "intelligence cycle."

To begin with, intelligence is always concerned with a *target*—the focus of the problem about which the customers want answers. The analyst's primary job is to develop a level of *understanding* of the target and communicate that understanding to the customer. In the *Star Wars* example, the target was the Death Star. The rebel intelligence effort supported operations by identifying its weak point and communicating that level of understanding to the customer.



Logic dictates that the intelligence process should revolve around how best to approach the target. That is exactly what the remainder of this book is concerned with: the steps to solving an intelligence problem, using a target-centric approach, and communicating *understanding* to the customer so that the customer can act based on that understanding. This process is different from that depicted in most introductory texts and courses, but it is the direction that intelligence is taking in practice. A brief review of the traditional intelligence cycle will illustrate why.

## The Traditional Intelligence Cycle

Intelligence has traditionally been described as following a series of steps called the *intelligence cycle*. Figure 3-1 illustrates the cycle in elementary form.

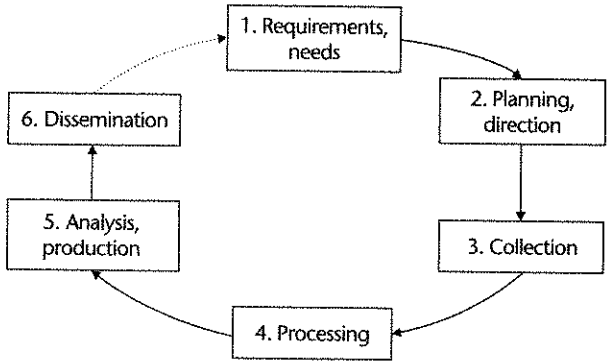
The cycle typically begins with a *requirements* or *needs* step, which amounts to a definition of the intelligence problem. Usually it takes the form of a rather general question from an intelligence customer, such as, "How stable is the government of Ethiopia?"

Then comes *planning*, or *direction*—determining how the other components of the cycle will address the problem. Collectors have to be tasked to gather missing bits of information. Analysts have to be assigned to do research and write a report on Ethiopian government stability.

The cycle then proceeds to *collection*, or gathering information. Ethiopian newspapers have to be acquired. Communications intelligence (COMINT) has to be focused on Ethiopian government communications. Human intelligence (HUMINT) operatives have to ask questions of sources with knowledge of Ethiopian internal affairs.

From there, the information has to be *processed*. Foreign language material must be translated. Encrypted signals must be decrypted. Film or digital signals must be translated into visible imagery. Responses from HUMINT sources must be validated and organized into a report format.

*Figure 3-1* The Traditional Intelligence Cycle



The newly collected and processed material must be brought together with relevant historical material to create intelligence in an *analysis* phase. An analyst must create outcome scenarios based on the current Ethiopian situation, generate profiles of Ethiopian leaders, and assess their likely responses to possible events. The analysis phase also typically includes a peer and supervisory review of the finished product, except in fast-moving, combat intelligence situations, in which simple fusion (discussed in chapter 18) is done.

The finished intelligence must be *disseminated* to the customer in a written report (usually sent electronically) or a briefing. Then comes a transition to new requirements or needs, and a new cycle begins.

Over the years the intelligence cycle has become almost a theological concept: No one questions its validity. Yet when pressed, many intelligence officers admit that the intelligence process "really doesn't work like that." In other words, effective intelligence efforts are not cycles. Here are some reasons why.

The cycle defines an *antisocial* series of steps that constrains the flow of information. It separates collectors from processors from analysts and too often results in "throwing information over the wall" to become the next person's responsibility. Everyone neatly avoids responsibility for the quality of the final product. Because such a compartmentalized process results in formalized and relatively inflexible requirements at each stage, it is more predictable and therefore more vulnerable to an opponent's countermeasures. In intelligence, as in most forms of conflict, if you can predict what your opponents will do, you can defeat them.

The cycle-defined view, when it considers the customer at all, tends to treat the customer in the abstract as a monolithic entity. The feedback loop inherent in a true cycle is absent; in practice, a gap exists between dissemination and needs. Customers, being outside the loop, cannot make their changing needs known. Why does this gap exist?

In government, intelligence officers and policymakers often are almost totally ignorant of one another's business.[2] In the military the gap may be less severe—the importance of intelligence has been ingrained in military culture over a long time. But as in the civilian side of government, an organizational demarcation usually exists. Most commanders and their staffs have not had intelligence assignments, and intelligence officers usually have not had operations assignments. They tend to speak different jargons, and their definitions of what is important in an operation differ. Military intelligence officers often know more about an opponent's capability than they do about their own unit's capability, and the commander often has the inverse problem.

In large intelligence organizations, such as those of the U.S. government, the collection element (see Figure 3-1) typically is well organized, well funded, and automated to handle high volumes of traffic. In contrast, the step wherein one moves from disseminated intelligence to new requirements is almost completely unfunded and requires extensive feedback from intelligence consumers. The system depends on the customers voicing their needs. Military organizations have a formal system for that to occur. Policymakers, with one important exception that is discussed in chapter 19, do not. The policymaker's input is largely informal, is dependent on feedback to the analyst, and often passes through several intermediaries. And for the newest class of customers of U.S. intelligence—law enforcement—the feedback is rudimentary. No entity has the clear responsibility to close the loop. Analysts and their managers, who typically have the closest ties to intelligence customers, usually determine customer needs. But it is too often a hit-or-miss proposition because it depends on the inclination of analysts who are dealing with other pressing problems.

The traditional conception of the intelligence cycle also prevails because it fits a conventional paradigm for problem solving. It flows logically from the precept that the best way to work on an intelligence problem is to follow a sequential, orderly, and linear process, working from the question (the problem) to the answer (the solution). One begins by understanding the question; the next step is to gather and analyze data. Analysis techniques are then applied to answer the question. This pattern of thinking is taught in the simplest problem-solving texts, and we use it almost instinctively. In fact, conventional wisdom says that the more complex the problem, the more important it is to follow this orderly flow. The flaw of this linear problem-solving approach is that it obscures the real, underlying cognitive process: The mind does not work linearly; it jumps around to different parts of the problem in the process of reaching a solution. In practice, intelligence officers might jump from analysis back to collection, then to requirements, to collection again, then back to analysis, in what seems a very untidy process, and which in no way resembles a cycle.

Despite its irrelevance to the real world of intelligence, the concept of an intelligence cycle persists. Some of the foremost experts in U.S. and British intelligence, such as former director of national intelligence Mike McConnell and noted British author Michael Herman, have questioned its relevance. Both McConnell[3] and Herman[4] noted that the so-called cycle is actually a collection of feedback loops. But old habits tend to fade very slowly, and so the intelligence cycle continues to be taught in introductory intelligence courses.

U.S. intelligence analysis guru Sherman Kent noted that the problems with the intelligence cycle—the compartmentation of participants, the gap between dissemination and needs, and the attempt to make linear a nonlinear process—are worse in large organizations and in situations far removed from the heat of conflict.[5] As Keith Hall, former director of the National Reconnaissance Office, observed, "During crisis the seams go away and all the various players pull together to create end-to-end solutions . . . but we don't do that well in a noncrisis situation."[6]

In summary, the traditional cycle may adequately describe the structure and function of an intelligence community, but it does not describe the intelligence process. In the evolving world of information technology, the traditional cycle may be even less relevant. Informal networks (communities of interest) increasingly are forming to address the problems that Kent identified and to enable a nonlinear intelligence process using secure web technology.

The cycle is still with us, however, because it embodies a convenient way to organize and manage intelligence communities like those in large governments and large military organizations. And it is in some respects a defensive measure; it makes it difficult to pinpoint responsibility for intelligence failures.

The cycle traces its lineage back to an automaker named Henry Ford. Over a century ago, Ford divided the labor by breaking the assembly of the Model T into eighty-four distinct steps. Each worker was trained to do just one of these steps. So you had interchangeable parts, division of labor, and a continuous flow of a standard product.

And it worked. The Model T had a remarkable run; first produced in 1908, it kept the same design until the last one, number 15,000,000, rolled off the line in 1927—something that hasn't happened since. Industry adopted the assembly line concept. Many governments did also. The Soviets built their entire system (industrial and consumer goods) on the Ford model. If you're producing one thing and demand is stable, it's efficient and easy to manage.

Fifty years ago, the automobile production "cycle" looked a lot like the traditional intelligence cycle. Marketing staff would come up with requirements for new cars. Designers would create a design and feed it to production. Production would retool the factory and produce the cars in a long assembly line. The cars came out at the end and went to a sales force that sold the cars to customers. And then marketing started on a new requirements set, beginning the cycle anew. No one had responsibility for the final result. Today automobile production is a team effort—with marketing, sales, design, and production staff sitting in the same room with consumer representatives, working together on a common target: the new automobile. This complex, interactive, collaborative, and social process results in the faster production of higher quality, more market-oriented products.

Finally, the "cycle" was designed to deal with the flow of reporting in cable or paper form. It provided an orderly, one-way flow. We set up intelligence organizations based entirely on slow flow of intelligence around the cycle. We kept that system even when first secure telephones, then secure computer communications, made it possible to speed things along. We even kept the name "production" as though we were building automobiles.

This book defines an alternative, interactive approach that is gaining currency in intelligence communities, for a world where intelligence problems will always be increasingly complex.

## Intelligence as a Target-Centric Process

An alternative to the traditional intelligence cycle is to make all stakeholders, *including customers*, part of the intelligence process. Stakeholders in the intelligence community include collectors, processors, analysts, and the people who plan for and build systems to support them. U.S. customers on a given issue could include, for example, the president, the National Security Council staff, military command headquarters, diplomats, the Department of Homeland Security, state or local law enforcement, and the commanders of U.S. naval vessels. To include them in the intelligence process, the cycle must be redefined, not for convenience of implementation in a traditional organizational hierarchy, but so that the process can take full advantage of evolving information technology and handle complex problems.



Figure 3-2 defines this *target-centric*, or objective-oriented, view of the intelligence process. Here the goal is to construct a shared picture of the target, from which all participants can extract the elements they need to do their jobs and to which all can contribute from their resources or knowledge, so as to create the most accurate target picture. It is not a linear sequence, nor is it a cycle (though it contains many feedback loops, or cycles); it is a *network process*, a social process, with all participants focused on the objective. It has been accurately described within the U.S. intelligence community as a "network-centric collaboration process."[7]

Letitia Long, while director of the National Geospatial-Intelligence Agency, endorsed the idea of a fresh approach that replaces the cycle. She termed it "sequence neutrality," observing that

> It turns the traditional TCPED (tasking, collection, processing, exploitation, and dissemination) process focused on a suite of fixed targets inside out. It allows the analyst to form a hypothesis first and then search the data and even drive new collection to test the hypothesis. It also allows the analyst to integrate data before exploitation to focus an analyst's investigation on anomalies in the data that have been correlated. Our ability to know the unknown depends on this new approach to collection and processing data.[8]

Subsequently, the U.S. intelligence community has implemented a concept very similar to the target-centric approach. Called "object-based production," or OBP, it involves organizing intelligence efforts around "objects" (targets) of intelligence interest. It features cloud-based sharing of the state of knowledge of the intelligence target. The sharing includes customers as well—policymakers, warfighters, and foreign partners.[9]

*Figure 3-2* A Target-Centered View of the Process

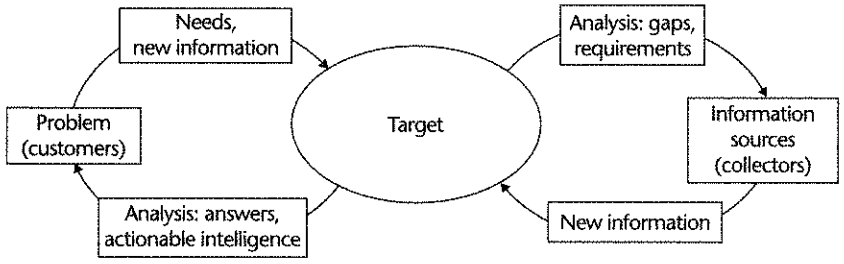


Figure 3-2 focuses on the role that all-source analysts must take in this new environment: pulling in customers. The analyst's job is to take inputs from many sources and provide support to many customers who have different timeline requirements and need different levels of analysis. The major characteristics of intelligence in today's environment are as follows:

- Analysis can take many forms and draw on many sources. It's common to draw on several sources to get a more complete picture. Extrinsic sources include specialized expertise from academia, social media, or industry.
- Analysis on any subject is a continuous process. Customers require intelligence support every day, some on shared issues, some on issues unique to them.
- Consequently, each of the steps in the intelligence process (collection, processing, exploitation, analysis, dissemination) is happening all the time on any given subject.

The traditional cycle wasn't designed to handle that environment. The target-centric approach is.

In the process depicted in Figure 3-2, customers who have operational problems look at the current state of knowledge about the target (the current target picture) and identify the information they need. Intelligence analysts, working with collectors who share the same target model, translate the needs into "knowledge gaps" or "information requirements" for the collectors to address. As collectors obtain the needed information, it is incorporated into the shared target model. From this picture, analysts extract actionable intelligence, which they provide to the customers, who may in turn add their own insights. They may also add new information needs.

Let us bring some meaning to the process shown in Figure 3-2: The date is December 2, 1993. Colombian police lieutenant Hugo Martinez watches the signal display on his computer screen and listens to his headphones as his police surveillance van moves through the streets of Medellin, Colombia. Electronic intelligence has traced the cell phone calls of drug kingpin Pablo Escobar to this neighborhood. Martinez is trying to find the exact house where a desperate Escobar is talking to his son about getting the family out of Colombia.

The signal on the computer screen and in the headphones strengthens and peaks. The van stops next to a house, and Martinez looks up to see a fat man standing at a window, holding a cell phone. The man turns away, and the cell phone conversation ends abruptly. Martinez reports to his commander: "I've got him located. He's in this house." The commander snaps out orders for all units to converge and surround the building. Five police officers force their way in the front door and exchange gunshots with the occupants. Ten minutes later, the gunfire stops. On the building rooftop, Pablo Escobar lies dead.[10]



This example, a true story, was the end of an intense cooperative effort between U.S. and Colombian intelligence officers that had endured for over a year. In this case, the intelligence effort had several customers—an operations team comprising the Colombian police, the U.S. Army support team in Colombia, and the Colombian and U.S. governments, each with different intelligence needs. The information sources included COMINT focused on Escobar's cell phones and those of his associates, HUMINT from Escobar's associates, and financial information from other sources. The operations team focused on finding Escobar; the intelligence analysts who supported them had a more extensive target that included Escobar's family, his business associates, his bankers, and his agents in the Colombian government. Escobar would not have been caught if the intelligence search had focused solely on him and had ignored his network.

In the Escobar case, as in other, less time-critical operations, intelligence analysis is implicit and pervasive. But it is not all done by analysts. The customers and the providers of information also participate and will do so whether the analyst welcomes it or not. Both customers and providers possess valuable insights about the target, and both want their insights included in the final analytic product. However, someone must make the process work: creating and maintaining the model of the target, eliciting customer needs and changing them into requirements for new information, accepting new information and incorporating it into the target model, and then extracting actionable intelligence and ensuring that it gets to the customer. All of these are functions that analysts have always performed. In the target-centric process, analysts still perform these functions, but collectors and customers cannot only see into the process but have more opportunity to contribute to it. The analyst's job becomes more like that of a process manager.

The team-generated model of the target is intended to facilitate and encourage interaction among collectors, analysts, and customers, who may be geographically remote from one another, via an electronic web. Because the team view is more interactive, or social, than the intelligence cycle view, it is a better way to handle complex problems. Because all participants share knowledge of the target, they are better able to identify gaps in knowledge and understand the important issues surrounding it. The team-generated view brings the full resources of the team to bear on the target. During U.S. operations in Afghanistan in 2002, intelligence officers used screens similar to Internet chat rooms to share data in an interactive process that in no way resembled the traditional intelligence cycle,[11] and they continued that successful pattern during Operation Iraqi Freedom. It now is an established method of producing tactical intelligence that is likely to be used in all future U.S. and coalition operations. But the method that has worked at the tactical level remains a work in progress at the national intelligence level.[12]

The target-centric approach is resilient. Because the participants collaborate, there is no single point of failure; another member of the network could step in to act as facilitator; and the whole team shares responsibility for the product.

The process is also able to satisfy a wide range of customers from a single knowledge base. There are usually many customers for intelligence about a given problem, and each customer has different needs. For example, military, foreign relations, financial, and foreign trade organizations all may need information about a specific country. Because there is a common target, their needs will overlap, but each organization also will have unique needs.

The target-centric approach has proven to work well for today's complex problems and issues. Though depicted as a cycle, the traditional process is in practice linear and sequential, whereas the target-centric process is collaborative by design. Its nonlinear analytic method allows for participation by all stakeholders, so that real insights into a problem can come from any knowledgeable source. Involving customers increases the likelihood that the resulting intelligence will be used. It also reminds the customers of (or introduces them to) the value of an analytic approach to complex problems. It has been asserted that in the United States, government has detached itself from the analytic process and relied too much on the intelligence community to do its analytic thinking.[13] Increasing policymakers' exposure to the analytic process could help reverse that trend.

The collaborative team concept also has the potential to address two important pressures that intelligence analysts face today:

- *The information glut.* Analysts are overloaded with incoming material from collectors. The team approach expands the team of analysts to include knowledgeable people from the collector, processor, and customer groups, each of whom can take a chunk of the information glut and filter out the irrelevant material. Business organizations have been doing this for years, and they now rely heavily on web-based private networks.
- *The customer demand for more detail.* All intelligence customers are demanding increasingly greater detail about targets. This should not be surprising given that targets are more networked and the range of the customer's options to deal with opponents using the DIME instruments has become richer. If the operations target is a building (such as an embassy or a command-and-control center), for example, intelligence may need to include the floor plan; the number of levels; whether it has a basement; the type of construction; roof characteristics; what type of heating, ventilation, and air conditioning it uses; when the building is empty; and so forth. Such details become critical when the objective is to place a smart bomb on the building or to take out the building's electric power.

For collaboration to work—for the extended team to share the data overload and provide the needed target detail—intelligence organizations have to provide incentives to share that outweigh the disincentives discussed in chapter 1. Team members have to have a wealth of mutual trust and understanding; both require team building and extended social interaction. Some companies have been highly successful at collaboration; the U.S. government is still working at it.

It is important to note also what the collaborative process is not. As Mark Lowenthal has stated, it is not a substitute for competitive analysis—the process by which different analysts present alternative views of the target.[14] Collaboration, properly handled, is intended to augment competitive analysis by ensuring that the competing views share as much information about the target as possible.

## The Target

In Norfolk, Virginia, a young intelligence officer controls a Predator unmanned aerial vehicle (UAV) on patrol over Afghanistan. The Predator's video display shows a vehicle racing along a mountain road. Moving the Predator closer for a better view, the officer identifies the vehicle as a BMP, a type of armored personnel carrier. He calls in an AC-130 Spectre gunship on patrol nearby. As the AC-130 appears on the scene, the BMP lurches to a stop. The rear doors open, and the BMP disgorges Taliban soldiers running for cover. The Spectre's guns open up. In the Predator's video, the soldiers crumple one by one as the stream of gunship fire finds them.

The intelligence officer was able to order the attack by the AC-130 Spectre gunship because he had a mental picture of potential Taliban targets, and the BMP fit the picture in its location and characteristics. The BMP in Afghanistan was a specific operations target; the intelligence view of the target was much larger. It included details of the road network in Afghanistan that could support the BMP and maps delineating areas of Taliban control. A good mental model is essential when intelligence provides such close support to operations. The intelligence officer is under intense pressure to distinguish quickly between a troop carrier and a bus full of villagers, and the consequences of an error are severe.

### *The Target as a Complex System*

As the BMP example suggests, the typical intelligence target is a *system*, not a single vehicle or building. Intelligence analysis therefore starts by thinking about the target in that fashion. A system comprises structure, function, and process, and the analyst has to deal with each of the three in systems thinking.[15] The *structure* is defined by a system's components and the relationships among them. *Function* involves the effects or results produced, that is, the outputs. *Process* refers to the sequence of events or activities that produce results. Chapter 9 discusses systems analysis in more detail.

The Escobar drug cartel is (or was) an example of a system. Figure 3-3 is a macro-level model of a cocaine cartel's structure, showing the major components and the relationships among them. Each of the components has a structure of its own, comprising subcomponents and their relationships. The coca supply component, for example, has subcomponents such as the farmers, land, seed, and farm equipment. A cocaine cartel also has several major functions, such as surviving in the face of state opposition, making a profit, and providing cocaine to its customers. Each component also has additional functions that it performs. The transportation and distribution infrastructure has the functions of getting cocaine from the processor to the customer, selling the drugs, and obtaining payment for them. As this example illustrates, most intelligence targets are systems that have subordinate systems, also called *subsystems*. The Escobar leadership comprised a subsystem whose structure included components such as security and finance; it had a function (managing the cocaine network) and a process for carrying it out.

As a counterexample, a geographic entity is not a system. A country, for example, is much too abstract a concept to be treated as a system. It does not have structure, function, or process, though it contains within it many systems that have all three. Consequently, a geographic entity could not be considered an intelligence target. The government of a region is a system—it has structure, function, and process.

Most intelligence targets are systems. Furthermore, most are *complex systems* because

- They are dynamic and evolving.
- They are nonlinear, in that they are not described adequately by a simple structure such as a tree diagram or the linear structure depicted in Figure 3-1 to illustrate the traditional intelligence cycle.

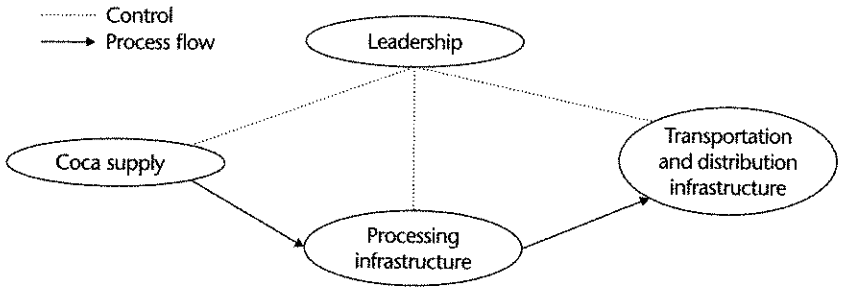
A cocaine supply network is a complex system. It is constantly evolving, and its intricate web of relationships does not yield easily to a hierarchical breakout. It can, however, usually be described as a network. Most complex systems of intelligence interest are, in fact, networks—the subject of the next section.

### *The Target as a Network*

Though intelligence has always targeted opposing systems, it has often tended to see them as individual, rather than connected, entities. Such a narrow focus downplays the connections among organizations and individuals—connections that can be the real strength or weakness of an opposing system taken as a whole. That is why we focus on networks, which are treated in detail in chapter 10.

Networks, by definition, comprise *nodes* with *links* between them. Several types of networks have been defined, and they vary in the nature of their nodes and links. In communications networks, the nodes are points, usually

*Figure 3-3* Example Target: Cocaine Network



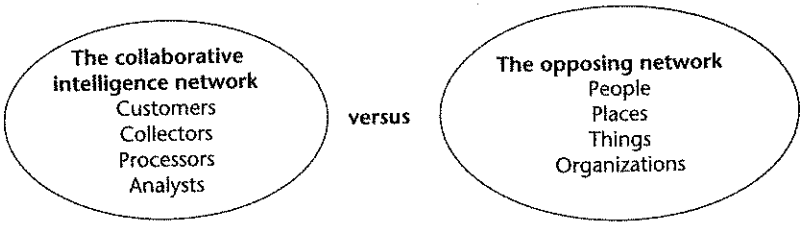

geographically separated, between which the communications are transmitted. A communications satellite and its ground terminals are communications nodes. The links are the communications means—for example, fiber optics, satellite communications, and wireless (cellular) telephones. In social networks, the nodes are people. The links show the relationships between people and usually the nature of those relationships. A social network exists, for example, at a cocktail party or in an investment club.

In this book, unless otherwise specified, *network* means a *target network* in which the nodes can be almost any kind of entity—people, places, things, concepts. A cocaine supply system is a target network. The links define relationships among the nodes. Sometimes the links quantify the relationship. Whereas communications networks and social networks are useful concepts in intelligence, the more powerful target network is a better concept for intelligence analysis and is widely used.

In intelligence, the opposing target network typically is some combination of governments; individuals; NGOs such as environmental, human rights, and religious groups; commercial firms; or illicit organizations, all tied together by some purpose, as suggested by the diagram in Figure 3-4. In conflicts, the goal of intelligence is to develop an understanding of the opposing network, so as to make the analyst's own network as effective as possible and render the opponent's network ineffective.

Analysts responsible for assessing the capabilities of an air defense network, a competing commercial firm or alliance, or a narcotics production and distribution network must take a network view. As an example, an analyst concerned with the balance of power in the Middle East might be tempted to look at Syria, Saudi Arabia, Iran, and Iraq separately. Yet no assessment of the future of the Middle East should ignore the continuing tensions among them—the constraining effects of past hostilities on any country's likely future actions and the opportunities that they provide for opponents. These individual countries are part of a larger target network bound by ties of mutual mistrust and suspicion.

*Figure 3-4* Netwar Competition: Network versus Network

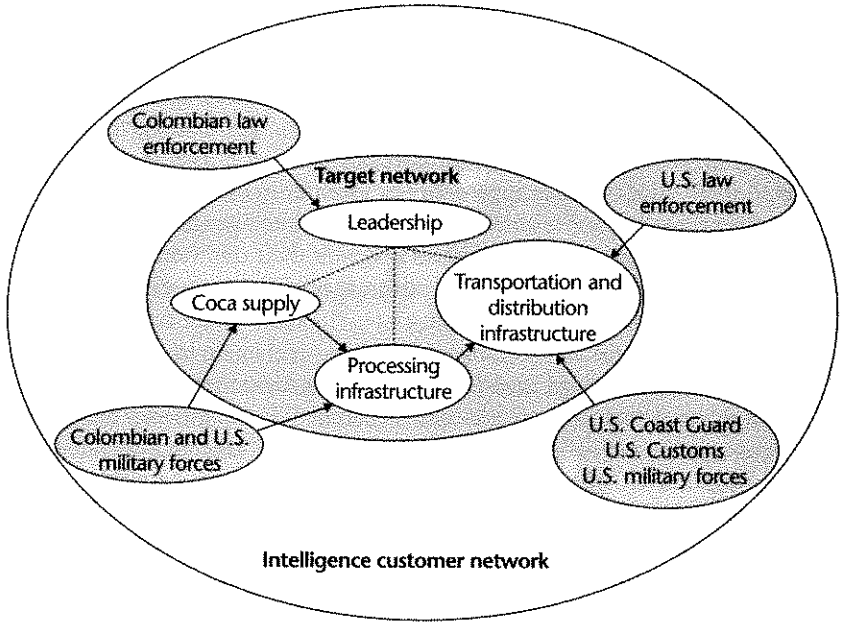



It is also important to look at both sides as networks. It may be easier, especially in a bureaucracy, to see the opponent's side as a network than to see that one's own intelligence and operational assets form a network and to fully exploit its strengths. General Stanley McChrystal, reflecting on his experiences in trying to make networks function effectively in Afghanistan, wrote that

> It takes a network to defeat a network. But fashioning ourselves to counter our enemy's network was easier said than done, especially because it took time to learn what, exactly, made a network different. As we studied, experimented, and adjusted, it became apparent that an effective network involves much more than relaying data. A true network starts with robust communications connectivity, but also leverages physical and cultural proximity, shared purpose, established decision-making processes, personal relationships, and trust. Ultimately, a network is defined by how well it allows its members to see, decide, and effectively act. But transforming a traditional military structure into a truly flexible, empowered network is a difficult process.[16]

The collaborative, collector-analyst-customer, target-centric approach creates an effective network to deal with the opposing network. Figure 3-5 shows the example of a cocaine supply target network and some components of the opposing (that is, U.S. and Colombian) intelligence customer network. As the figure indicates, it makes sense that U.S. law enforcement would target the transportation and distribution infrastructure, because much of that infrastructure is located within U.S. borders. U.S. law enforcement would not normally be able to target the cartel leadership in Colombia. Colombian law enforcement, by contrast, could target both the cartel leadership and its processing infrastructure, but it would probably find the leadership a more profitable target. The customer network shown in the figure is far from complete, of course; it might include political leadership in the United States and Colombia, for example, or regional and European government entities concerned about the cocaine trade.

*Figure 3-5* Netwar Example against a Cocaine Network




Chapter 2 introduced the concepts of netwar and the network target. Within the U.S. Department of Defense netwar has been referred to as *network-centric warfare*.[17] Defense planners have identified three themes:

- A shift in perspective from the single-node target to the network target
- A shift from viewing actors as independent to viewing them as part of a continuously adapting system
- A focus on making strategic choices to adapt—or merely to survive—in the changing system

Network-centric warfare is not a new concept in the business world.[18] Companies such as Royal Dutch Shell were creating networks of this kind, including allied outsiders, three decades ago. Participants in that network found it a powerful mechanism for bringing a wide range of expertise to bear on problems.[19] The World Wide Web has speeded the formation of such networks, and the network-centric approach has been adopted widely in the commercial world. Companies such as Cisco Systems and Wal-Mart have made the collaborative network a key part of their business strategies. In Wal-Mart's network-centric retailing approach, the company shares sales information with suppliers in near-real time so that they can better control production

and distribution, as well as manage their own supply chains for Wal-Mart products.[20] Another example is the network-centric securities trading system Autobahn, created by Deutsche Morgan Grenfell.[21] Autobahn replaces the traditional, trader-centered (hierarchical) system of securities trading with a network system in which participants have equal access to securities pricing information. The advantage that the network-centric approach gives companies such as Wal-Mart and Deutsche Morgan Grenfell is that it forces their competitors to adopt similar approaches or lose out in competition.

Business intelligence is ahead of government intelligence in applying the netwar strategy. Even military organizations, with their traditions of hierarchical structure, seem to be adopting the advantages of the network structure, as General McChrystal's earlier quote illustrates. In cases when national intelligence efforts must deal with commercial entities, as they do in economic matters, weapons proliferation, and funds-laundering cases, intelligence analysts increasingly understand network-centric conflict. Furthermore, NGOs are becoming more involved in military, economic, political, and social issues worldwide, and NGO involvement usually makes any conflict network-centric, as it did with the Zapatistas in Mexico.

Any discussion of the network target should touch on *the* intelligence target of the past decade: Osama bin Laden. In person, he was a hard target to miss, being 6'5" tall and possessing a physical description that was well known throughout the world. But from 2001 to 2011, bin Laden proved to be an elusive target, almost impossible to find if considered alone. However, like Pablo Escobar, he had to run a large network and, of course, have some form of communication with it. Despite bin Laden's very good security system, intelligence analysts and collectors focused on the network as a target and were able to pinpoint his location in Abbottabad, Pakistan, in 2010–2011. The result was the SEAL Team 6 raid on May 2, 2011, that resulted in bin Laden's death.

It was a telling example of netwar in action. Even so, that it took nearly ten years for the allied intelligence services to track down bin Laden illustrates the importance of making the intelligence network as inclusive as possible. The opposing network, unfortunately, included significant elements of the Pakistani government that supported bin Laden, making allied intelligence operations in Pakistan more difficult.

### *Spatial and Temporal Attributes of the Target*

In addition to being a system and a network, targets of intelligence interest typically have spatial and temporal attributes, and analysis must take these into account. Chapter 11 goes into detail on analyzing these attributes.

Many targets of intelligence interest are fixed geographically. These are mostly elements of a region's infrastructure. Cities and towns, lines of communication (roadways and railways), and installations all have fixed locations. The intelligence interest here is in determining their location (usually in coordinates for smaller targets) or their position on a map for lines of communication.



Many targets of interest, though, are mobile. People, ships, vehicles in general, and satellites all move in space. They may be in one place for a while, but they generally have to be characterized in both space and time.

And even fixed targets such as factories have events occurring around them, or change physically in some way. A missile silo or an airfield, for example, is fixed. But patterns of activity around the silo or airfield may indicate that something of intelligence interest is occurring. So we have to analyze even the fixed targets spatially and temporally.

## Summary

Intelligence, when supporting policy or operations, is always concerned with a target. Traditionally, intelligence has been described as a cycle: a process starting from requirements, to planning or direction, collection, processing, analysis and production, dissemination, and then back to requirements. That traditional view has several shortcomings. It separates the customer from the process and intelligence professionals from one another. A gap exists in practice between dissemination and requirements. The traditional cycle is useful for describing structure and function and serves as a convenient framework for organizing and managing a large intelligence community. But it does not describe how the process works or should work.

Intelligence is in practice a nonlinear and target-centric process, operated by a collaborative team of analysts, collectors, and customers collectively focused on the intelligence target. The rapid advances in information technology have enabled this transition.

All significant intelligence targets of this target-centric process are complex systems in that they are nonlinear, dynamic, and evolving. As such, they can almost always be represented structurally as dynamic networks—opposing networks that constantly change with time. In dealing with opposing networks, the intelligence network must be highly collaborative. Historically, however, large intelligence organizations, such as those in the United States, provide disincentives to collaboration. If those disincentives can be removed, U.S. intelligence will increasingly resemble the most advanced business intelligence organizations in being both target-centric and network-centric.

Targets of intelligence interest have spatial attributes: They exist somewhere in space at a given instant. They also have temporal attributes: They move around or change as time passes. Identifying the target's location and monitoring its movements or other changes are important elements of the target-centric approach to intelligence.

Having defined the target, the first question to address is, What do we need to learn about the target that our customers do not already know? This is the intelligence problem, and for complex targets, the associated intelligence issues are also complex. The next chapter discusses how to define the intelligence issue.

## Notes

1. A *dead drop* is a temporary concealment place for material that is in transit between two clandestine intelligence operatives who cannot risk a face-to-face meeting. A tin can next to a park bench or the interior of a personable robot are classic examples of dead drops.
2. David Kennedy and Leslie Brunetta, "Lebanon and the Intelligence Community," Case Study C15-88-859.0 (Cambridge, Mass.: Kennedy School of Government, Harvard University, 1988).
3. William J. Lahneman, *The Future of Intelligence Analysis*, Center for International and Security Studies at Maryland, Final Report, Vol. I (March 10, 2006), E-8.
4. Michael Herman, *Intelligence Power in Peace and War* (Cambridge, U.K.: Cambridge University Press, 1996), 100.
5. Quoted in Sherman Kent, "Producers and Consumers of Intelligence," in *Strategic Intelligence: Theory and Application*, 2nd ed., ed. Douglas H. Dearth and R. Thomas Goodden (Washington, D.C.: U.S. Army War College and Defense Intelligence Agency, 1995), 129.
6. Stew Magnuson, "Satellite Data Distribution Lagged, Improved in Afghanistan," *Space News*, September 2, 2002.
7. V. Joseph Broadwater, "I Would Make the T-PED Pain Go Away," memorandum for the record (U.S. National Reconnaissance Office, Washington, D.C., August 3, 2000, photocopy).
8. Letitia A. Long, "Activity-Based Intelligence: Understanding the Unknown," *Intelligencer: Journal of U.S. Intelligence Studies* (Fall/Winter 2013): 9.
9. Defense Intelligence Agency, "Modernizing Defense Intelligence: Object Based Production and Activity Based Intelligence" (briefing graphic), June 27, 2013, http://www.slideshare.net/RDSWEB/dia-activity-basedintelligence.
10. Mark Bowden, "A 15-Month Manhunt Ends in a Hail of Bullets," *Philadelphia Inquirer*, December 17, 2000.
11. Magnuson, "Satellite Data Distribution."
12. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, http://www.wmd.gov/report/wmd_report.pdf, 14.
13. Robert D. Steele, "The New Craft of Intelligence," February 1, 2002, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=217.
14. Mark M. Lowenthal, "Intelligence Analysis," address to the Intelligence Community Officers' Course at CIA University, July 19, 2002.
15. Jamshid Gharajedaghi, *Systems Thinking: Managing Chaos and Complexity* (Boston: Butterworth-Heinemann, 1999), 110.
16. General (Retired) Stanley McChrystal, "It Takes a Network," *Foreign Policy*, February 21, 2011.
17. Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute*, 124, no. 1 (1998): 28–35.
18. Liam Fahey, *Competitors* (New York: Wiley, 1999), 206.
19. Peter Schwartz, *The Art of the Long View* (New York: Doubleday, 1991), 90.
20. James F. Moore, *The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems* (New York: HarperBusiness, 1996).
21. Cebrowski and Garstka, "Network-Centric Warfare."

# 4

# *Defining the Intelligence Issue*

*A problem well stated is a problem half solved.*

Inventor Charles Franklin Kettering

The preceding chapter focused on the intelligence target—in most cases, a complex network. For such targets, there are typically several people who are interested in receiving intelligence. And these customers typically have different interests or different intelligence problems to which they want answers. The U.S. Department of Energy might be interested in Iraqi oil well activity to estimate current production; a field military commander might be interested in the same oil well activity to prevent the wellheads from being sabotaged. Therefore, all intelligence analysis efforts start with some form of problem definition.

The initial guidance that customers give analysts about an issue, however, almost always is incomplete, and it may even be unintentionally misleading. Thomas Fingar, drawing on his experience as chairman of the National Intelligence Council, cites a number of examples of flawed issue statements:

- In one case, intelligence customers were monitoring the progress of a program to protect Iraqi oil pipelines. They were pleased to note that no attacks had occurred on one pipeline segment—until an intelligence analyst posed the question that should have been part of the problem statement: Was that segment operational during the period in question? It turned out that the segment had been out of commission.[1]
- In another case, Fingar received a request from the National Security Council staff for an update on political reconciliation, economic reconstruction, and public safety in Iraq. Probing for details about this seemingly straightforward request, Fingar found that the staff director really wanted to know whether an NSC assumption—that progress on political reconciliation would facilitate progress in other areas—was supported by the evidence. (It was not.)[2]

Therefore, the first and most important step an analyst can take is to understand the issue in detail. He or she must determine why the intelligence analysis is being requested and what decisions the results will support. The success of analysis depends on an accurate issue definition. As one senior policy customer noted in commenting on intelligence failures, "Sometimes, what they [the intelligence officers] think is important is not, and what they think is not important, is."[3]

The poorly defined issue is so common that it has a name: the *framing effect*. It has been described as "the tendency to accept problems as they are presented, even when a logically equivalent reformulation would lead to diverse lines of inquiry not prompted by the original formulation."[4] We encounter it in many disciplines where the problem must be defined properly before it can be solved effectively. The classic example of framing was a 1982 study in which U.S. doctors were presented with two different formulations for the outcome of an operation. One set of doctors was informed that the operation had a 93 percent survival rate; the other set was told that the operation had a 7 percent mortality rate. Rationally, there should have been no difference in the doctors' decisions, since both statistics have the same meaning. But the doctors showed a definite preference not to operate when they were quoted a mortality rate instead of a survival rate.[5] Intelligence analysts often run afoul of the framing effect—one of the best-known examples being the National Intelligence Council's estimate on the Iraqi weapons of mass destruction program discussed in Appendix I.

For these reasons, veteran analysts go about the analysis process quite differently than do novices. At the beginning of a task, novices tend to attempt to solve the perceived customer problem immediately. Veteran analysts spend more time thinking about it to avoid the framing effect. They use their knowledge of previous cases as context for creating mental models to give them a head start in addressing the problem. Veterans also are better able to recognize when they lack the necessary information to solve a problem,[6] in part because they spend enough time at the beginning, in the problem definition phase. In the case of the complex problems discussed in this chapter, issue definition should be a large part of an analyst's work.

Issue definition is the first step in a process known as *structured argumentation*. We'll get into the details of structured argumentation in chapter 7. For now, the important thing to understand is that structured argumentation always starts by breaking down a problem into parts so that each part can be examined systematically.[7]

## Statement of the Issue

In the world of scientific research, the guidelines for problem definition are that the problem should have "a reasonable expectation of results, believing that someone will care about your results and that others will be able to build upon them, and ensuring that the problem is indeed open and underexplored."[8]



Intelligence analysts should have similar goals in their profession. But this list represents just a starting point. Defining an intelligence analysis issue begins with answering five questions:

- *When is the result needed?* Determine when the product must be delivered. (Usually, the customer wants the report yesterday.) In the traditional intelligence process, many reports are delivered too late—long after the decisions have been made that generated the need—in part because the customer is isolated from the intelligence process. Also, tight deadlines are increasingly a challenge in all areas of intelligence; the customer values having precise and detailed intelligence in real time. The target-centric approach can dramatically cut the time required to get actionable intelligence to the customer because the customer is part of the process.
- *Who is the customer?* Identify the intelligence customers and try to understand their needs. The traditional process of communicating needs typically involves several intermediaries, and the needs inevitably become distorted as they move through the communications channels. Also, even if the intelligence effort is done for a single customer, the results often go to many other recipients. It helps to keep in mind these second-order customers and their needs, as well.
- *What is the purpose?* Intelligence efforts usually have one main purpose. This purpose should be clear to all participants when the effort begins and also should be clear to the customer in the result. The main purpose, for instance, might be to provide intelligence to support trade negotiations between the United States and the European Union. A number of more specific intelligence purposes support this main purpose—such as identifying likely negotiating tactics and pinpointing issues that might split the opposing negotiators. Again, customer involvement helps to make the purpose clear to the analyst.
- *What form of output, or product, does the customer want?* Written reports (now in electronic form) are standard in the intelligence business because they endure and can be distributed widely. When the result goes to a single customer or is extremely sensitive, a verbal briefing may be the form of output. Briefings have the advantage of customer interaction and feedback, along with a certainty that the intended recipient gets the message. Studies have shown that customers never read most written intelligence.[9] Subordinates may read and interpret the report, but the message tends to be distorted as a result. So briefings or (ideally) constant customer interaction with the intelligence team during the target-centric process helps to get the message through.
- *What are the real questions?* Obtain as much background knowledge as possible about the problem behind the questions the customer asks, and understand how the answers will affect organizational decisions.

The purpose of this step is to narrow the problem definition. A vaguely worded request for information is usually misleading, and the result will almost never be what the requester wanted.

Be particularly wary of a request that has come through several "nodes" in the organization. The layers of an organization, especially those of an intelligence bureaucracy, will sometimes "load" a request as it passes through with additional guidance that may have no relevance to the original customer's interests. A question that travels through several such layers often becomes cumbersome by the time it reaches the analyst. A question about the current Israeli balance of payments, for example, could wind up on the analyst's desk as instructions to prepare a complete assessment of the Israeli economy. In such situations, the analyst must go back to the originator of the request and close the loop. The problem of the corrupted communications channel is so pervasive in intelligence that it is covered in detail in chapter 7.

The request should be specific and stripped of unwanted excess. This entails focused (and perhaps repeated) interaction with the customer responsible for the original request—the executive, the policymaker, or the operations officer. Ask the customer if the request is correctly framed. The time spent focusing the request saves time later during collection and analysis. It also makes clear what questions the customer does *not* want answered—and that should set off alarm bells, as the next example illustrates.

When the United States was involved in Lebanon in 1983, U.S. policymakers did not want to hear from U.S. intelligence that there was no reasonable way to force Syrian president Hafez Al-Assad to withdraw from Lebanon.[10] The result of this disconnect between intelligence and the customer was a foreign policy debacle for the United States. On October 23, 1983, terrorists blew up the Marine barracks at Beirut International Airport with a truck bomb that killed 241 Marines. The United States subsequently withdrew from Lebanon.

Policymakers can sometimes choose not to be informed by intelligence on selected issues, as they did in Lebanon. If the issue is important enough, though, the analyst has to find a way to deal with that choice. Chapter 19 discusses how to respond when the customer is antipathetic to intelligence.

After answering these five questions, the analyst will have some form of problem statement. On large (multiweek) intelligence projects, this statement will itself be a formal product. The issue definition product helps explain the real questions and related issues. Once it is done, the analyst will be able to focus more easily on answering the questions that the customer wants answered.

## The Issue Definition Product

When the final intelligence product is to be a written report, the issue definition product is usually in précis (summary, abstract, or terms of reference) form.



The précis should include the problem definition or question, notional results or conclusions, and assumptions. For large projects, many intelligence organizations require the creation of a concept paper or outline that provides the stakeholders with agreed terms of reference in précis form.

If the intelligence product is to be a briefing, a set of graphics will become the final briefing slides. If possible, the slides should be turned into a notional briefing (that is, a briefing with assumptions, notional results, and conclusions) and shown to the customer; this approach will improve the chances that the final report will address the issues in the customer's mind.

Either exercise will help all participants (customers, collectors, and analysts) understand their assignments or roles in the process. Think of it as a going-in position; no one is tied to the précis or notional presentation if the analysis later uncovers alternative approaches—as it often does.

Whether the précis approach or the notional briefing is used, the issue definition should conclude with an issue decomposition view.

## Issue Decomposition

The basic technique for defining a problem in detail has had many names. Nobel laureate Enrico Fermi championed the technique of taking a seemingly intractable problem and breaking it into a series of manageable subproblems. The classic problem that Fermi posed for his students was, "How many piano tuners are there in Chicago?" The answer could be reached by using the sort of indirect approach that is common in the intelligence business: by estimating how many families were in the city, how many families in the city per piano, and how many pianos a tuner can tune a year.[11] Glenn Kent of RAND Corporation uses the name *strategies-to-task* for a similar breakout of U.S. Defense Department problems.[12] Within the U.S. intelligence community, it is sometimes referred to as *problem decomposition* or "decomposition and visualization."

Whatever the name, the process is simple: Deconstruct the highest level abstraction of the issue into its lower-level constituent functions until you arrive at the lowest level of tasks that are to be performed or subissues to be dealt with. In intelligence, the deconstruction typically details issues to be addressed or questions to be answered. Start from the problem definition statement and provide more specific details about the problem. The process defines intelligence needs from the top level to the specific task level via *taxonomy*—a classification system in which objects are arranged into natural or related groups based on some factor common to each object in the group. At the top level, the taxonomy reflects the policymaker's or decision maker's view and reflects the priorities of that customer. At the task level, the taxonomy reflects the view of the collection and analysis team. These subtasks are sometimes called key intelligence questions (KIQs) or essential elements of information (EEIs).

The issue decomposition approach has an instinctive appeal. We naturally tend to form hierarchical social arrangements and to think about issues hierarchically. Issue decomposition follows the classic method for problem solving.

It results in a requirements, or needs, hierarchy that is widely used in intelligence organizations. A few examples from different national policy problem sets will help to illustrate the technique.

Figure 4-1 shows part of an issue decomposition for political intelligence on a given country or region of the world. For simplicity, only one part of the decomposition is shown down to the lowest level.

Figure 4-1 illustrates the importance of taking the decomposition to the lowest appropriate level. The top-level question, "What is the political situation in Region *X*?" is difficult to answer without first answering the more specific questions lower down in the hierarchy, such as "What progress is being made toward reform of electoral systems?"

Another advantage of the hierarchical decomposition is that it can be used to evaluate how well intelligence has performed against specific issues or how future collection systems might perform. Again referring to Figure 4-1, it is difficult to evaluate how well an intelligence organization is answering the question, "What is the political situation in Region *X*?" It is much easier to evaluate the intelligence unit's performance in researching the transparency, honesty, and legitimacy of elections, because these are very specific issues.

Obviously there can be several different issues associated with a given intelligence target or several different targets associated with a given issue. If the request is for an overall assessment of a country's economy, rather than its political situation, then the decomposition might look very much like that shown in Figure 4-2. Because of space limitations, the bottom of the figure shows only four of thirteen question sets. At the bottom level, issues

*Figure 4-1* Political Situation Issue Decomposition

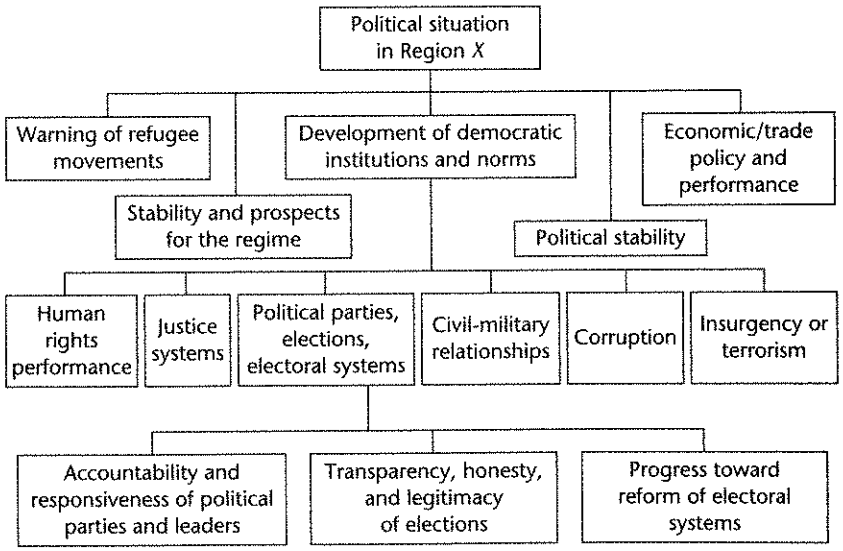
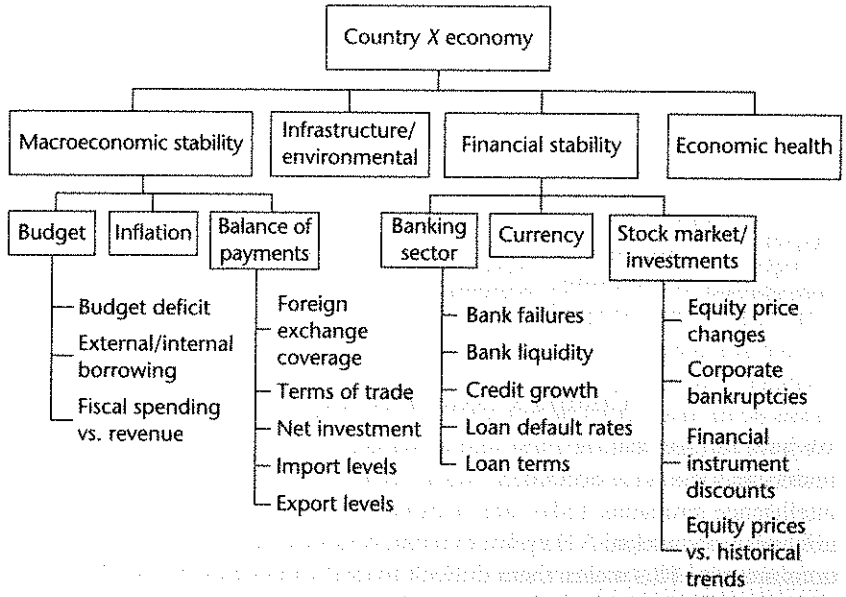



*Figure 4-2* Country *X* Economic Issue Decomposition

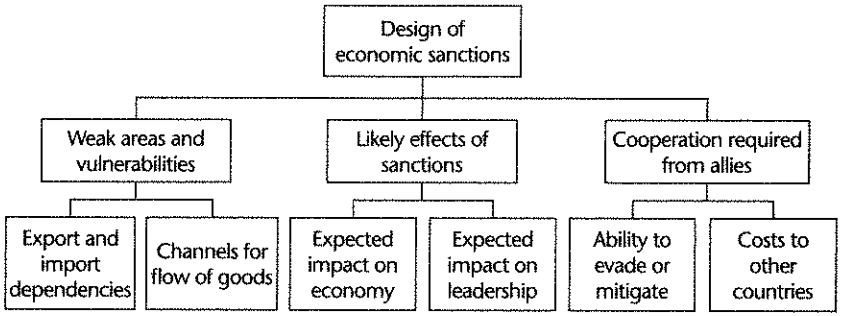



such as terms of trade and corporate bankruptcies can be addressed with relative ease, compared with high-level questions such as "What is country *X*'s financial stability?"

These two issue decompositions are examples of the sorts of issues that intelligence analysts typically encounter about a target, and both are oriented to broad information needs (here, political and economic). But the decomposition can be much more specific and more oriented to the customer's options for attacking the problem. Figure 4-3 illustrates an example—intelligence support to the design of economic sanctions against a country, the type that might have been used to design sanctions against Iraq during the 1990s. An intelligence analyst might have difficulty in directly answering this question from a policymaker: "Tell me what I need to know to develop economic sanctions against country *X*." So the analyst would create a decomposition of the issue and answer more specific questions such as, "What impact will sanctions have on the economy?" and integrate the answers to provide an answer to the top-level question.

No matter how narrow the top-level intelligence task, it can likely be broken out into an array of specific questions. If the job is to assess the capabilities of an opponent's main battle tank, then an analyst would consider the tank's speed, range, armor, and firepower. Maintenance requirements, quality of crew training, logistics, and command and control supporting the tank should also be examined. Without these less obvious components, the tank is simply an expensive piece of metal and a threat to no one.

*Figure 4-3* Economic Sanctions Issue Decomposition




## Complex Issue Decomposition

We have learned that the most important step in the intelligence process is to understand the issue accurately and in detail. Equally true, however, is that intelligence problems today are increasingly complex—often described as nonlinear, or "wicked." They are dynamic and evolving, and thus their solutions are, too. This makes them difficult to deal with—and almost impossible to address within the traditional intelligence cycle framework. A typical example of a wicked issue is that of a drug cartel—the cartel itself is dynamic and evolving and so are the questions being posed by intelligence consumers who have an interest in it.

A typical real-world customer's issue today presents an intelligence officer with the following challenges:[13]

- *It represents an evolving set of interlocking issues and constraints.* Only by working through the problem to get answers can one understand the ramifications. Often even when the project is complete, an analyst finds out from the customer that he or she didn't fully appreciate the issues involved. The narcotics example has an evolving set of interlocking issues and constraints. Take the constraints on possible solutions: Selectively introducing poison into the narcotics supply to frighten consumers and kill demand might reduce drug use, but it is not an acceptable option for the United States.
- *There are many stakeholders—people who care about or have something at stake in how the issue is resolved.* (Again, this makes the problem-solving process a fundamentally social one, in contrast to the antisocial traditional intelligence cycle.) The contraband narcotics problem has many stakeholders on both sides of the problem. Among the stakeholders trying to eliminate contraband narcotics are the Drug Enforcement Agency, law enforcement, U.S. customs, the military, U.S. banks, and governments in drug-producing countries. The opposing side's stakeholders include the cartel, its supporters in the foreign government, the financial institutions that it uses for funds laundering, farmers, processors, intermediaries, street forces, and drug users. And the stakeholders each have different perspectives. Consider the Pablo Escobar example from chapter 3. From the U.S. point of view, the problem was to stem the flow of narcotics into the United States. From the Colombian government point of view, the problem was stopping the assassinations and bombings that Escobar ordered.
- *The constraints on the solution, such as limited resources and political ramifications, change over time.* The target is constantly changing, as the Escobar example illustrates, and the customers (stakeholders) change their minds, fail to communicate, or otherwise change the rules of the game. Colombians didn't want high-visibility "gringos" involved in the hunt for Escobar, though they relaxed this constraint as they gained confidence in the U.S. operatives.[14] The U.S. government didn't want to be associated with killings of Escobar's relatives, business associates, and lawyers. The result is that the issue definition is dynamic; it cannot be created once and left unchanged.
- *Because there is no final issue definition, there is no definitive solution.* The intelligence process often ends when time runs out, and the customer must act on the most currently available information. Killing Escobar did not solve the narcotics problems of the United States or Colombia. Instead the rival Cali cartel became the dominant narcotics supplier in Colombia—an example of an unintended consequence.



Harvard professor David S. Landes summarized these challenges nicely when he wrote, "The determinants of complex processes are invariably plural and interrelated."[15] Because of this—because complex or wicked problems are an evolving set of interlocking issues and constraints, and because the introduction of new constraints cannot be prevented—the decomposition of a complex problem must be dynamic; it will change with time and circumstances. As intelligence customers learn more about the targets, their needs and interests will shift.

Ideally, a complex issue decomposition should be created as a network because of the interrelationship among the elements. In Figure 4-1 the "political stability" block is related to all three of the lowest blocks under "political parties, elections, and electoral systems," though they all appear in different parts of the hierarchy; political stability being enhanced, for example, when elections are transparent, honest, and legitimate. In Figure 4-3, "Ability to evade or mitigate" sanctions is clearly related to "Expected impact on economy" or "Expected impact on leadership," though they also are in different parts of the hierarchy. Iraq's ability to evade or mitigate sanctions during the 1990s was sufficient to minimize the impact on its leadership but insufficient to keep the Iraqi economy healthy. If lines connected all of the relationships

that properly exist within these figures, they would show very elaborate networks. The resulting dynamic network becomes quite intricate and difficult to manage at our present stage of information technology development.

Although the hierarchical decomposition approach may be less than ideal for complex problems, it works well enough if it is constantly reviewed and revised during the analysis process. It allows analysts to define the issue in sufficient detail and with sufficient accuracy so that the rest of the process remains relevant. There may be redundancy in a linear hierarchy, but the human mind can usually recognize and deal with the redundancy. To keep the decomposition manageable, analysts should continue to use the hierarchy, recognizing the need for frequent revisions, until information technology comes up with a better way.

## Structured Analytic Methodologies for Issue Definition

Throughout the book we discuss a class of analytic methodologies that are collectively referred to as *structured analytic methodologies* or SATs. This book does not attempt to cover all of the many techniques that have been described. Issue decomposition, discussed earlier, is the most relied upon such technique for defining an intelligence issue. But two other SATs are valuable in this process as well: brainstorming and a key assumptions check.

### *Brainstorming*

Brainstorming is commonly used in problem solving to stimulate fresh thinking. In intelligence, it can be applied in any part of the analysis process as an aid to thinking. But it is most useful in the issue definition stage at the start of an analysis project to help generate a range of hypotheses.[16] A variant of brainstorming, called *starbursting*, is derived from the idea of a six-pointed star with each point labeled with one of the words *who, what, when, where, why,* and *how*. The technique is to brainstorm by asking questions about the intelligence problem—questions that start with one of these six words.[17]

One caution about brainstorming, though. Texts on the subject usually warn not to allow criticism during the exercise. A flawed premise of brainstorming, which has been popular for over sixty years, is that criticism inhibits original thinking. Studies have shown that the opposite is true: More original ideas and fresh approaches come from team efforts when criticism is encouraged rather than suppressed.[18] So it may be more effective to allow critiques during the session. The key is to create a climate up front in which participants understand they are on the same team and that all ideas, including debate, no matter how seemingly far out, contribute to a better final product.

Brainstorming is supposed to be a group activity. But there should be no lower limit to the number of people in a brainstorming group. If it's difficult to pull together a group, brainstorming still can be an effective tactic with two people. Many a successful enterprise has begun when two people with a cocktail napkin start drawing models while they exchange ideas. And starbursting—asking the six questions—can be done by one person, if necessary.

The goal is to stimulate new thinking, especially about hypotheses. Getting that result is more important than following a defined set of rules.

### *Key Assumptions Check*

As noted earlier in this chapter, assumptions form a part of the issue definition. So it is important to conduct a key assumptions check during this process. A key assumption is a hypothesis that (a) has been accepted as true and (b) will be a part of the problem definition or the final assessment product. A pitfall occurs when those assumptions are not questioned or doubted at the beginning of an analysis effort, and become simply accepted as fact thereafter.

The purpose of this check then is to identify any key assumptions, question their validity and relevance, and state them explicitly only after they have been accepted. The process begins with the statement of each assumption. Then, an analyst must ask why the assumption is valid and whether it remains valid in all circumstances.

Finally, a relevancy check needs to be done. To be "key," an assumption must be essential to the analytic reasoning that follows it. That is, if the assumption turns out to be invalid, then the conclusions also probably are invalid. CIA's *Tradecraft Primer* identifies several questions that need to be asked about key assumptions:

- How much confidence exists that this assumption is correct?
- What explains the degree of confidence in the assumption?
- What circumstances or information might undermine this assumption?
- Is a key assumption more likely a key uncertainty or key factor?
- Could the assumption have been true in the past but less so now?
- If the assumption proves to be wrong, would it significantly alter the analytic line? How?
- Has this process identified new factors that need further analysis?[19]

## Example: Defining the Counterintelligence Issue

To illustrate, let's take an example of an issue that has all of the challenges listed in this chapter: that of counterintelligence.

Remember: It is easy to begin with a wrong definition of the issue. If that happens, and if the definition is not revised as discussed herein, then the best analysis in the world will not avert a bad outcome. In fact, the counterintelligence issue has been poorly addressed in many countries for many years because the effort to do so began from a wrong issue definition that was never reconsidered.

Counterintelligence (CI) in government usually is thought of as having two subordinate problems: security (protecting sources and methods) and catching spies (counterespionage). CI posters, literature, and briefings inevitably focus

on the spies caught—probably because their primary purpose is to discourage treason. In doing so, they're also catering to the popular media perception of counterintelligence.

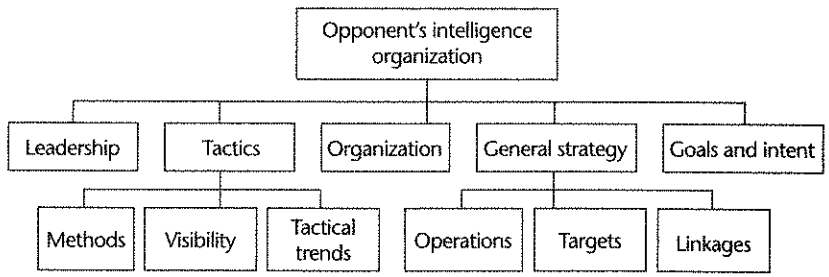
If the issue is defined this way—security and counterespionage—the response in both policy and operations is defensive. Personnel background security investigations are conducted. Annual financial statements are required of all employees. Profiling is used to detect unusual patterns of computer use that might indicate computer espionage. Cipher-protected doors, badges, personal identification numbers, and passwords are used to ensure that only authorized persons have access to sensitive intelligence. The focus of communications security is on denial, typically by encryption. Leaks of intelligence are investigated to identify their source.

But whereas the focus on security and counterespionage is basically defensive, the first rule of strategic conflict is that *the offense always wins*. So, for intelligence purposes, you're starting out on the wrong path if the issue decomposition starts with managing security and catching spies. The Iraqi WMD Commission recognized this flawed approach when it observed that U.S. counterintelligence has been criticized as being focused almost exclusively on counter-HUMINT, that is, on catching spies.[20]

A better issue definition approach starts by considering the real target of counterintelligence: the opponent's intelligence organization. Good counterintelligence requires good analysis of the hostile intelligence services. As we will see in several examples later in this book, if you can model an opponent's intelligence system, you can defeat it. So we start with the target as the core of the problem and begin an issue decomposition. Figure 4-4 illustrates the result: a simple first-level issue decomposition.

If the counterintelligence issue is defined in this fashion, then the counterintelligence response will be forward-leaning and will focus on managing foreign intelligence perceptions through a combination of covert action, denial, and deception. The best way to win the CI conflict is to go on the offensive (model the target, anticipate the opponent's actions, and defeat him or her). Instead of denying information to the opposing side's intelligence

*Figure 4-4* Counterintelligence Issue Decomposition




machine, for example, you feed it false information that eventually degrades the leadership's confidence in its intelligence services.

To do this, one needs a model of the opponent's intelligence system that can be subjected to target-centric analysis, including its communications channels and nodes, its requirements and targets, and its preferred sources of intelligence. How one uses such a model is discussed in the next chapter.

## Summary

Before beginning intelligence analysis, the analyst must understand the customer's issue. This usually involves close interaction with the customer until the important issues are identified. The problem then has to be deconstructed in an issue decomposition process so that collection, synthesis, and analysis can be effective.

All significant intelligence issues, however, are complex and nonlinear. The complex problem is a dynamic set of interlocking issues and constraints with many stakeholders and no definitive solution. Although the linear issue decomposition process is not an optimal way to approach such problems, it can work if it is reviewed and updated frequently during the analysis process.

Along with decomposition, two other structured analytic methodologies are useful for issue definition. Brainstorming stimulates fresh thinking about the issue. Its variant, starbursting, has participants ask questions that start with *who, what, when, where, why,* and *how*.

Issue definition is the first step in a process known as structured argumentation. As an analyst works through this process, he or she collects and evaluates relevant information, fitting it into a target model (which may or may not look like the issue decomposition); this part of the process is discussed in chapters 5–7. The analyst identifies information gaps in the target model and plans strategies to fill them—the subject of chapter 20. The analysis of the target model then provides answers to the questions posed in the issue definition process. The next chapter discusses the concept of a model and how it is analyzed.

## Notes

1. 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), 10.
2. Ibid.
3. Stew Magnuson, "Satellite Data Distribution Lagged, Improved in Afghanistan," *Space News*, September 2, 2002, 6.
4. Matthew Herbert, "The Intelligence Analyst as Epistemologist," *International Journal of Intelligence and CounterIntelligence*, 19, no. 4 (December 2006): 666–684.
5. Barbara J. McNeill, Stephen G. Paulker, and Amos Tversky, "On the Framing of Medical Decisions," in *Decision Making: Descriptive, Normative, and Prescriptive Interactions*, ed. David E. Bell, Howard Raiffa, and Amos Tversky (Cambridge, U.K.: Cambridge University Press, 1988), 562–568.

6. Rob Johnson, *Analytic Culture in the US Intelligence Community* (Washington, D.C.: Center for the Study of Intelligence, CIA, 2005), 64.
7. Jill Jermano, *Introduction to Structured Argumentation*, DARPA Project Genoa Technical Report, May 2002.
8. Robert W. Lucky, "In Research, the Problem is the Problem," *IEEE Spectrum* (July 2011): 30.
9. Jack Davis, *Intelligence Changes in Analytic Tradecraft in CIA's Directorate of Intelligence* (Washington, D.C.: CIA Directorate of Intelligence, April 1995), 2.
10. David Kennedy and Leslie Brunetta, "Lebanon and the Intelligence Community," Case Study C15-88-859.0 (Cambridge, Mass.: Kennedy School of Government, Harvard University, 1988), 15.
11. Hans Christian von Baeyer, *The Fermi Solution* (Portland, Ore.: Random House, 1993).
12. Glenn Kent and William Simon, *New Challenges for Defense Planning: Rethinking How Much Is Enough* (Santa Monica, Calif.: RAND, 1994).
13. E. Jeffrey Conklin, "Wicked Problems and Fragmentation," CogNexus Institute, March 24, 2003, www.cognexus org/wpf/wickedproblems.pdf.
14. Mark Bowden, "Martinez Pushes Ahead with the Hunt," *Philadelphia Inquirer*, December 3, 2000.
15. David S. Landes, *The Wealth and Poverty of Nations* (New York: Norton, 1998), 577.
16. CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, D.C.: Author, March 2009), 27.
17. Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, D.C.: CQ Press, 2011), 102.
18. Jonah Lehrer, "Groupthink," *New Yorker*, January 30, 2012, 22–27.
19. CIA, *A Tradecraft Primer*, 7.
20. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, chapter 11.

# 5

# *Conceptual Frameworks for Intelligence Analysis*

*If we are to think seriously about the world, and act effectively in it, some sort of simplified map of reality . . . is necessary.*

Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order*

The introduction in chapter 1 stressed that analysis must have a conceptual framework for crafting the analytic product. "Balance of power," for example, was an important conceptual framework used by policymakers during the Cold War. A different conceptual framework has been proposed for assessing the influence that one country can exercise over another.[1] This chapter describes a two-step general conceptual framework for applying the target-centric approach. The first step is to view the target from specific analytic perspectives. The second is to create a model of the target. Let's start with the perspectives.

## Analytic Perspectives—PMESII

In chapter 2, we discussed the instruments of national power—an *actions* view that defines the diplomatic, information, military, and economic (DIME) actions that executives, policymakers, and military or law enforcement officers can take to deal with a situation.

The customer of intelligence may have those four "levers" that can be pulled, but intelligence must be concerned with the *effects* of pulling those levers. Viewed from an effects perspective, there are usually six factors to consider: political, military, economic, social, infrastructure, and information, abbreviated *PMESII*. "Social" and "infrastructure" are not considered actions that can be taken but are in the category of *effects* of actions.[2] So which construct you use depends on whether you're thinking about