PART I

THE PROCESS, THE PARTICIPANTS, AND THE PRODUCT

Part I describes what intelligence is all about: the setting in which intelligence is created, how it is conducted and how it should be conducted, the people who develop and use it, and the distinct types of intelligence. Chapters 1 and 2 establish the setting. Chapter 3 introduces two views of the process: one based on the traditional intelligence cycle, and a more current view, the target-centric approach. After this overview, the remainder of part I discusses the participants in the process, beginning with the most important one in chapter 4: the customer. Chapter 5 considers the qualities and roles of the intelligence analyst, and chapter 6 details the analytic environment, with emphasis on the team that supports the creation of quality intelligence for the customer. Part I concludes with chapter 7, a discussion of intelligence products and cautions to consider.

1 INTRODUCTION

Intelligence analysis long existed in the shadows. When it appeared in early films and novels, the focus was on covert action rather than clandestine collection. The plotlines rarely focused on analysis—a boring subject, from the viewpoint of the storyteller. Even the nongovernment version, competitive intelligence[1] analysis, remained a subject to be avoided. Companies simply didn't talk about their intelligence efforts and the topic certainly didn't appear in popular media.

In the past two decades, that has changed. The discipline has emerged from the shadows, in part as the result of two trends. First has been the *commercialization of intelligence*. Much raw intelligence is now available from companies that provide imagery and signals intelligence from satellites and drones. Second, and a consequence of the first, is often described as the *globalization of intelligence*; intelligence analysis now has reached beyond its national level and military origins, and is practiced in homeland security, law enforcement, and commercial organizations around the globe. Intelligence has become known as more than spying and covert actions. And in the process, many participants have discovered that intelligence analysis is anything but boring. In fact, its practice often most closely resembles a Sherlock Holmes adventure.

But where Sherlock Holmes inevitably came up with the right answer, intelligence analysis sometimes misses the mark. And, as noted in the preface, we tend to learn more from our failures than from our successes. There is much to be learned from what have been called the two major US intelligence failures of this century—the September 11, 2001, attack on US soil and the subsequent miscall on Iraqi weapons of mass destruction. We'll cover both events later on; but let's begin with an overview of why we sometimes miss the mark.

WHY INTELLIGENCE FAILS

As a reminder that intelligence failures are not uniquely a US problem, it is worth recalling notable setbacks encountered by other countries in the past century:

- *Operation Barbarossa, 1941.* Josef Stalin acted as his own intelligence analyst, and he proved to be a very poor one. Russia was unprepared for a war with Nazi Germany, so Stalin ignored the mounting body of incoming intelligence indicating that the Germans were preparing a surprise attack. German

deserters who told the Russians about the impending attack were considered provocateurs and shot on Stalin's orders. When the attack, named Operation Barbarossa, came on June 22, 1941, Stalin's generals were surprised, their forward divisions trapped and destroyed.[2]

- *Singapore, 1942*. In one of the greatest military defeats that Britain ever suffered, 130,000 well-equipped British, Australian, and Indian troops surrendered to 35,000 weary and ill-equipped Japanese soldiers. On the way to the debacle, British intelligence failed in a series of poor analyses of their Japanese opponent, such as underestimating the capabilities of the Japanese Zero fighter aircraft and concluding that the Japanese would not use tanks in the jungle. The Japanese tanks proved highly effective in driving the British out of Malaya and back to Singapore.[3]

- *Yom Kippur, 1973*. Israel is regarded as having one of the world's best intelligence services. But in 1973, its leadership was closely tied to the Israeli cabinet and often served as both policy advocate and information assessor. Furthermore, Israel's past military successes had led to a degree of hubris and belief in inherent Israeli superiority. Israel's leaders considered their overwhelming military advantage a deterrent to their opponents. They also assumed that Egypt needed to rebuild its air force and forge an alliance with Syria before striking. In this atmosphere, Israeli intelligence was vulnerable to what became a successful Egyptian deception operation. Relying on these assumptions, Israel's chief of military intelligence dismissed reporting that correctly predicted the impending attack. The Israeli Defense Forces were caught by surprise when, without a rebuilt air force and having kept their agreement with Syria secret, the Egyptians launched an assault during Yom Kippur, the most important of the Jewish holidays, on October 6, 1973. The attack was ultimately repulsed, but only at a high cost in Israeli casualties.[4]

- *Falkland Islands, 1982*. Argentina wanted Great Britain to relinquish the Falkland Islands, which Britain had occupied and colonized in 1837. Britain's tactic was to conduct prolonged diplomatic negotiations without giving up the islands. There was abundant evidence of Argentine intent to invade, including a report of an Argentine naval task force headed for the Falklands with a marine amphibious force. But the British Foreign and Commonwealth Office did not want to face the possibility of an attack because it would be costly to deter or repulse. Britain's Latin America Current Intelligence Group (dominated at the time by the Foreign and Commonwealth Office) concluded accordingly, on March 30, 1982, that an invasion was not imminent. Three days later, Argentine marines landed and occupied the Falklands, provoking the British to assemble a naval task force and retake the islands.[5]

- *Afghanistan, 1979–1989.* The Soviet Union invaded Afghanistan in 1979 to support the existing Afghan government, which was dealing with an open rebellion. The Soviet decision to intervene was based largely on flawed intelligence provided by KGB chairman Yuri Andropov. Andropov controlled the flow of information to the general secretary of the Communist Party, Leonid Brezhnev, who was partially incapacitated and ill for most of 1979. KGB reports from Afghanistan created a picture of urgency and strongly emphasized the possibility that Afghan prime minister Hafizullah Amin had links to the CIA and US subversive activities in the region.[6] The conflict developed into a pattern in which the Soviets occupied the cities while the opposing forces, the mujahedeen, conducted a guerrilla war and controlled about 80 percent of the country. The mujahedeen were assisted by the United States, Pakistan, Saudi Arabia, the United Kingdom, Egypt, and the People's Republic of China. As the war dragged on, it saw an influx of foreign fighters from Arab countries, eager to wage jihad against the Soviet infidels. Among these fighters was a young Saudi named Osama bin Laden, who later would gain notoriety in another conflict. Faced with increasing casualties and costs of the war, the Soviets began withdrawing in 1987 and were completely out of the country by 1989, in what has been called the "Soviet Union's Vietnam War."

The common theme of these cases and others like them discussed in this book is *not* the inability to collect intelligence. In each of these cases, it had been collected. Three themes are common in all of them: failure to share information, failure to analyze collected material objectively, and failure of the customer to act on intelligence.

Failure to Share Information

From Pearl Harbor to 9/11 to the erroneous intelligence estimate on Iraq's possession of weapons of mass destruction (WMD), the inability or unwillingness of collectors and analysts to share intelligence was emblematic.

The Iraqi WMD Commission (the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, which issued its formal report to President George W. Bush in March 2005) found that collectors and analysts failed to work as a team.[7] They did not share information effectively. Progress has been made since then; however, the root causes for the failure to share remain in almost all intelligence services worldwide:

- Sharing requires openness. But any organization that requires secrecy to perform its duties will struggle with and often reject openness.[8] Most governmental intelligence organizations, including the US intelligence community, place more emphasis on secrecy than on effectiveness.[9] The penalty

for producing poor intelligence usually is modest. The penalty for improperly handling classified information can be career-ending.[10] There are legitimate reasons not to share; the US intelligence community has lost many collection assets because details about them were shared too widely. A balancing act is required between protecting assets and acting effectively in the world.

- Experts on any subject have an information advantage, and they tend to use that advantage to serve their own agendas.[11] Collectors and analysts are no different. At lower levels in the organization, hoarding information may confer job security benefits. At senior levels, unique knowledge may help protect the organizational budget. The natural tendency is to share the minimum necessary to avoid criticism and still protect the most valuable material. Any bureaucracy has a wealth of tools for hoarding information, and this book discusses the most common of them.
- Finally, both collectors and analysts find it easy to be insular. They are disinclined to draw on resources outside their own organizations.[12] Communication across organizations has long-term payoffs in access to intelligence from other sources, but in the short term, it requires more time and effort.

Although collectors, analysts, and intelligence organizations have a number of incentives to conceal information, leaders since 9/11 have acknowledged that intelligence must be a team sport. But effective teams require cohesion, formal and informal communication, cooperation, shared mental models, and similar knowledge structures—all of which contribute to sharing of information. Without such a common process, any team—especially the interdisciplinary teams that are necessary to deal with today's complex problems—will fall apart quickly.[13] Today's intelligence analysts, acting as project managers, are on the forefront in managing the required components and processes for sharing, a topic discussed in chapter 5.

Failure to Analyze Collected Material Objectively

In each of the cases of failure cited earlier, intelligence analysts or national leaders were locked into a *mindset*—a consistent thread in analytic failures. Louis Pasteur warned about that trap in his profession when he observed that "the greatest derangement of the mind is to believe in something because one wishes it to be so."

Mindset can manifest itself in the form of many biases and preconceptions, a short list of which would include the following:

- *Ethnocentric bias* involves projecting one's own cultural beliefs and expectations onto others. It leads to the creation of a "mirror-image" model, which looks at others as one looks at oneself, and to the assumption that others will act "rationally" as rationality is defined in one's own

culture. The Yom Kippur attack was not predicted because, from Israel's point of view, it was irrational for Egypt to attack without extensive preparation. Similarly, Soviet analysis of social processes in Afghanistan was done through the bias of Marxist-Leninist doctrine, which blinded the leadership to the realities of traditional tribal society and Islamic culture.[14] Put simply, Afghanistan did not fit into the ideological constructs of the Soviet leadership.[15]

- *Wishful thinking* involves excessive optimism or the avoidance of unpleasant choices. The British Foreign Office did not predict an Argentine invasion of the Falklands because, despite intelligence evidence that an invasion was imminent, they did not want to deal with it. Stalin made an identical mistake for the same reason prior to Operation Barbarossa. In Afghanistan, Soviet political and military leaders expected to be perceived as a progressive anti-imperialist force and were surprised to discover that the Afghans regarded the Soviets as foreign invaders and infidels.[16]
- *Parochial interests* cause organizational loyalties or personal agendas to affect the analysis process. That mindset was apparent in Andropov's shaping of the reporting that Brezhnev received about Afghanistan: Andropov wanted to see the USSR intervene there.
- *Status quo biases* cause analysts to assume that events will proceed along a straight line. The safest weather prediction, after all, is that tomorrow's weather will be like today's. An extreme case is the story of the British intelligence officer who, on retiring in 1950 after forty-seven years' service, reminisced: "Year after year the worriers and fretters would come to me with awful predictions of the outbreak of war. I denied it each time. I was only wrong twice."[17] The status quo bias causes analysts to fail to catch a change in the pattern.
- *Premature closure* results when analysts make early judgments about the answer to a question and then, often because of ego, defend the initial judgments tenaciously. This can lead the analyst to select (usually without conscious awareness) subsequent evidence that supports the favored answer and to reject (or dismiss as unimportant) evidence that conflicts with it. Israel's chief intelligence officer did exactly that in 1973.

These mindsets, if not challenged, will lead to poor assumptions and bad intelligence.

Failure of the Customer to Act on Intelligence

In some cases, as in Operation Barbarossa and the Falkland Islands incursion, the customer failed to understand or make use of the available intelligence.

A senior State Department official once remarked, half in jest, "There are no policy failures; there are only policy successes and intelligence failures."[18] The remark rankles intelligence officers, but it should be read as a call to action. Intelligence analysts shoulder partial responsibility when their customers fail to make use of the information provided. Analysts must meet the challenge of engaging the customer during the analysis process and help ensure that the resulting intelligence is accepted and considered when the customer must act.

In this book, considerable discussion is devoted to the vital importance of analysts being able to assess and understand their customers and their business or field. The collaborative, *target-centric approach* to intelligence analysis demands a close working relationship among all stakeholders, including the customer, as the means to gain the clearest conception of needs and the most effective results or products. Some chapters also illuminate ways to ensure that the customer considers the best available intelligence when making decisions.

Intelligence analysts have often been reluctant to closely engage one class of customer—the policymakers. In its early years, the CIA attempted to remain aloof from its policy customers to avoid losing objectivity in the national intelligence estimates process.[19] The disadvantages of that separation became apparent, as analysis was not addressing the customers' current interests and, therefore, was becoming less useful to policymaking. During the 1970s, CIA senior analysts began to expand contacts with policymakers. As both the Falklands and Yom Kippur examples illustrate, such closeness has its risks. In recent years, however, research has shown that analysts are able to work closely with policymakers and to make intelligence analyses relevant without losing objectivity.

WHAT THE BOOK IS ABOUT

This book describes a process for successful intelligence analysis that avoids the three themes of failure just outlined. All intelligence analysis depends on following a process that is based on a *conceptual framework* for crafting the analytic product.[20] In fact, all problem solving depends on starting from a conceptual framework,[21] and intelligence is about problem solving.

In addition to being an organizing construct, conceptual frameworks sensitize analysts to the underlying assumptions in their analysis and enable them to better think through complex problems.[22] Conceptual frameworks also are essential in identifying the target—which intelligence may be better equipped (or willing) to do than customers.

This book is about that process and conceptual framework. It develops the ideas of defining the intelligence issue, creating a model of the intelligence target, and extracting useful information from that model. All analysts naturally do this. The key to making it work is to *share* the model with collectors of information and customers of intelligence.

While all analysis follows that basic process, within that process and framework many tools have been developed to deal with specific disciplines and issues. These generally are referred to as *analytic methodologies* or *techniques*.

First, in contrast to the conceptual framework, no standard analytic methodology exists in the US intelligence community. Any large intelligence community is made up of a variety of disciplines, each with its own analytic methodology.[23] Furthermore, intelligence analysts routinely generate ad hoc methods to solve specific problems. This individualistic approach to analysis has resulted in a wide variety of analytic methods, more than 160 of which were identified in 2005 as available to US intelligence analysts.[24]

There are understandable reasons for the proliferation of methods. Methodologies are developed to handle very specific problems, and they are often unique to a discipline, such as economic or scientific and technical (S&T) analysis (which probably has the largest collection of problem-solving methodologies). As an example of how methodologies proliferate, after the Soviet Union collapsed, economists who had spent their entire professional lives analyzing a command economy were suddenly confronted with free market prices and privatization. No model existed anywhere for such an economic transition, and analysts had to devise from scratch methods to, for example, gauge the size of Russia's private sector.[25]

Second, an analyst's toolset also includes standard, widely used analytic techniques. An effective analyst must have a repertoire of them to apply in solving complex problems. They might include pattern analysis, trend identification, literature assessment, and statistical analysis. A number of these are presented throughout the book.

A few techniques, though, are used across all the analytic subdisciplines. They are called *structured analytic techniques*, or SATs. SATs are taught in most courses on intelligence analysis. Their use, however, has resulted in some criticism. For instance, as one author notes,

> *The problem is that many SATs stunt broad thinking and the kind of analysis that busy policymakers want. At the same time, single-minded attention to technique runs the risk of reducing analyses to mechanical processes that require only crunching of the "right" data to address policymaker needs.*[26]

Furthermore, as one senior intelligence officer has observed, "a reliance on structured analytic techniques does not necessarily produce better results" and that "blind faith in SATs is no more redemptive than any other blind faith."[27] Consequently, research indicates that SATs are seldom used in at least some parts of the US intelligence community.[28]

Despite the criticisms, SATs can have value in analysis if used at the right point in the process. The challenge is that novices can become overwhelmed by the number of SATs, and uncertain where to apply them in the process. And many are not commonly used by intelligence analysts, in part because they're cumbersome and time consuming

to apply. In this book, the focus is on the most useful SATs, and they are introduced at the point where they should be applied. SATs are not discussed in detail herein, as they are well covered in other texts.[29]

Sherman Kent, who is generally regarded as the father of US intelligence analysis, noted that an analyst has three wishes: "To know everything. To be believed. And to exercise a positive influence on policy."[30] This book will not enable an analyst to know everything; that is why we will continue to need estimates. But it should help analysts to learn or refine their tradecraft of analysis, and it is intended to help them toward the second and third wishes as well.

SUMMARY

Intelligence failures have three common themes that have a long history:

- Failure of collectors and analysts to share information. Good intelligence requires teamwork and sharing.
- Failure of analysts to objectively assess the material collected. The consistent thread in these failures is a mindset, primarily biases and preconceptions that hamper objectivity.
- Failure of customers to accept or act on intelligence. This lack of response is not solely the customer's fault. Analysts have an obligation to ensure that customers not only receive the intelligence but also fully understand it.

This book is about an intelligence process that can reduce such failures. The process begins with establishing a conceptual framework for analyzing any intelligence issue, followed by the application of analytic tools to deal with the issue.

A large intelligence community develops many such tools, comprising analytic methodologies and techniques, to deal with the variety of issues that it confronts. Structured analytic techniques may be the most valuable when properly applied. But the tools all work within a fundamental process: defining the intelligence issue, creating a model of the intelligence target, and extracting useful information from that model. Success comes from sharing the target model with all stakeholders.

NOTES

1. Large corporations typically have a staff that provides management with intelligence about competitors' plans, technologies, and products—called, not surprisingly, *competitive intelligence*.
2. John Hughes-Wilson, *Military Intelligence Blunders* (New York, NY: Carroll and Graf, 1999), 38.

3. Ibid., 102.
4. Ibid., 218.
5. Ibid., 260.
6. Svetlana Savranskaya, ed., "The Soviet Experience in Afghanistan: Russian Documents and Memoirs," National Security Archive, October 9, 2001, https://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB57/soviet.html.
7. Overview, *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, https://fas.org/irp/offdocs/wmd_report.pdf.
8. Rob Johnson, *Analytic Culture in the U.S. Intelligence Community* (Washington, DC: Center for the Study of Intelligence, CIA, 2005), xvi.
9. Ibid., 11.
10. There exists some justification for the harsh penalty placed on improper use of classified information; it can compromise and end a billion-dollar collection program or cut short the life of a dedicated and valued agent.
11. Steven D. Leavitt and Stephen J. Dubner, *Freakonomics* (New York, NY: HarperCollins, 2005), 13.
12. Johnson, *Analytic Culture*, 29.
13. Ibid., 70.
14. Savranskaya, "The Soviet Experience in Afghanistan."
15. Ibid.
16. Ibid.
17. Amory Lovins and L. Hunter Lovins, "The Fragility of Domestic Energy," *Atlantic Monthly*, November 1983, 118.
18. William Prillaman and Michael Dempsey, "Mything the Point: What's Wrong with the Conventional Wisdom about the C.I.A.," *Intelligence and National Security* 19, no. 1 (March 2004): 1–28.
19. Harold P. Ford, *Estimative Intelligence* (Lanham, MD: University Press of America, 1993), 107.
20. Itai Shapira, "Strategic Intelligence as an Art and a Science: Creating and Using Conceptual Frameworks," *Intelligence and National Security* 35 (no. 2): 283–99.
21. Shapira, "Strategic Intelligence as an Art and a Science."
22. Jason U. Manosevitz, "Needed: More Thinking about Conceptual Frameworks for Analysis—The Case of Influence," *Studies in Intelligence* 57, no. 4 (December 2013): 22, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-57-no-4/pdfs/Manosevitz-Focusing Conceptual%20Frameworks-Dec2013.pdf.
23. Johnson, *Analytic Culture*, xvii.
24. Manosevitz, "Needed: More Thinking about Conceptual Frameworks for Analysis – The Case of Influence."

25. Gerald K. Haines and Robert E. Leggett, eds., "Watching the Bear: Essays on CIA's Analysis of the Soviet Union," CIA Center for the Study of Intelligence Conference, Princeton University, March 2001, 8, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/.

26. Ibid.

27. Joseph W. Gartin, "The Future of Analysis," *Studies in Intelligence*, vol 63, no. 2 (2019).

28. Michael Landon-Murray. "Putting a Little More "Time" into Strategic Intelligence Analysis," *International Journal of Intelligence and CounterIntelligence*, 30:4, 785–809 (2017).

29. For two very good examples, see CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, DC: Author, March 2009), and Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, DC: CQ Press, 2011).

30. George J. Tenet, "Dedication of the Sherman Kent School." *CIA News & Information*, May 4, 2000, https://www.cia.gov/news-information/speeches-testimony/2000/dci_speech_05052000.html.