1

Introduction

The greatest derangement of the mind is to believe in something because one wishes it to be so.

Louis Pasteur

We learn more from our failures than from our successes. As noted in the preface to this book, there is much to be learned from what have been called the two major U.S. intelligence failures of this century—the September 11, 2001, attack on U.S. soil and the miscall on Iraqi weapons of mass destruction. So this book begins with an overview of why we sometimes fail.

Why Intelligence Fails

As a reminder that intelligence failures are not uniquely a U.S. problem, it is worth recalling some failures of other intelligence services in the past century:

- *Operation Barbarossa, 1941.* Josef Stalin acted as his own intelligence analyst, and he proved to be a very poor one. He was unprepared for a war with Nazi Germany, so he 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.[1]
- *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.[2]

- *Yom Kippur, 1973.* Israel is regarded as having one of the world's best intelligence services. But in 1973 the intelligence 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 certain amount of hubris and belief in inherent Israeli superiority. Israel's leaders considered their overwhelming military advantage a deterrent to attack. They assumed that Egypt needed to rebuild its air force and forge an alliance with Syria before attacking. In this atmosphere, Israeli intelligence was vulnerable to what became a successful Egyptian deception operation. The chief intelligence officer of the Israeli Southern Command suppressed an Israeli intelligence officer's report that correctly predicted the impending attack. The Israeli Defense Force was caught by surprise when, *without* a rebuilt air force and having kept their agreement with Syria secret, the Egyptians launched an attack on 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.[3]
- *Falkland Islands, 1982.* Argentina wanted Great Britain to hand over 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 Argentine 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.[4]
- *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 V. Andropov. Andropov controlled the flow of information to General Secretary 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 Prime Minister Hafizullah Amin had links to the Central Intelligence Agency (CIA) and U.S. subversive activities in the region.[5]

  The conflict developed into a pattern in which the Soviets occupied the cities while the opposing forces, called 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 and many other intelligence failures discussed in this book is *not* the failure to collect intelligence. In each of these cases, the intelligence had been collected. Three themes are common in intelligence failures: 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 estimate on Iraq's possession of weapons of mass destruction (WMD), the inability or unwillingness of collectors and analysts to share intelligence has been a recurring cause of failure.

Intelligence has to be a team sport. 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 complex problems of today—will quickly fall apart.[6]

Nevertheless, 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 effectively share information. And though progress has been made in the past decade, the root causes for the failure to share remain, in the U.S. intelligence community as well as 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 U.S. 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 U.S. intelligence community has lost many collection assets because details about them were too widely shared. So it comes down to a balancing act between protecting assets and acting effectively in the world. Commercial organizations are more effective at intelligence sharing because they tend to place more emphasis on effectiveness than on secrecy; but they also have less risk of losing critical sources from compromises.

- 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 have job security benefits. At senior levels, unique knowledge may help protect the organizational budget. So the natural tendency is to share the minimum necessary to avoid criticism and to 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 of intelligence and analysts find it easy to be insular. They are disinclined to draw on resources outside their own organizations.[12] Communication takes time and effort. It has long-term payoffs in access to intelligence from other sources, but few short-term benefits.

In summary, collectors, analysts, and intelligence organizations have a number of incentives to conceal information and not enough benefits to share it. Despite the pressures of U.S. intelligence community leaders to be more collaborative, the problem is likely to persist until the incentives to share outweigh the benefits of concealment.

Failure to Analyze Collected Material Objectively

In each of the cases cited at the beginning of this introduction, intelligence analysts or national leaders were locked into a *mindset*—a consistent thread in analytic failures. Falling into the trap that Louis Pasteur warned about in the observation that begins this chapter, they believed because, consciously or unconsciously, they wished 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 on 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. Afghanistan did not fit into the ideological constructs of the Soviet leadership. Their 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.[13]
- *Wishful thinking* involves excessive optimism or avoiding unpleasant choices in analysis. The British Foreign Office did not predict an Argentine invasion of the Falklands because, in spite of intelligence evidence that an invasion was imminent, they did not want to deal with it. Josef 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.[14]
- *Parochial interests* cause organizational loyalties or personal agendas to affect the analysis process.
- *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."[15] 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.

All of these mindsets can lead to poor assumptions and bad intelligence if not challenged. And as the Iraqi WMD Commission report notes, analysts often allow unchallenged assumptions to drive their analysis.[16]

Failure of the Customer to Act on Intelligence

In some cases, as in Operation Barbarossa and the Falkland Islands affair, the intelligence 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."[17] 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 intelligence provided. Analysts have to meet the challenge of engaging the customer during the analysis process and help ensure that the resulting intelligence is accepted and taken into account when the customer must act.

In this book I devote considerable discussion to the vital importance of analysts' being able objectively to assess and understand their customers and their customers' business or field. The first part of the book describes the collaborative, "target-centric" approach to intelligence analysis that 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 discuss ways to ensure that the customer takes into account 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.[18] The disadvantages of that separation became apparent, as analysis was not addressing the customer's current interests, and intelligence 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. But in many cases analysts have been able to work closely with policymakers and to make intelligence analyses relevant without losing objectivity.

What the Book Is About

This book develops a process for successful intelligence analysis—including avoiding the three themes of failure we've just covered.

Studies have found that no baseline standard analytic method exists in the U.S. intelligence community. Any large intelligence community is made up of a variety of disciplines, each with its own analytic methodology.[19] Furthermore, intelligence analysts routinely generate ad hoc methods to solve specific analytic problems. This individualistic approach to analysis has resulted in a great variety of analytic methods, more than 160 of which have been identified as available to U.S. intelligence analysts.[20]

There are good reasons for this 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.[21]

But all intelligence analysis methods derive from a fundamental process. This book is about that process. It develops the idea of creating a model of the intelligence target and extracting useful information from that model. These two steps—the first called "synthesis" and the second called "analysis"—make up what is known as intelligence analysis. All analysts naturally do this. The key to avoiding failures is to *share* the model with

collectors of information and customers of intelligence. There are no universal methods that work for all problems, but a basic process does exist.

Also, analysis has to have a conceptual framework for crafting the analytic product. This text defines a general conceptual framework for all types of intelligence problems. In addition to being an organizing construct, it has been argued that conceptual frameworks sensitize analysts to the underlying assumptions in their analysis and enable them to better think through complex problems.[22]

There also are standard, widely used analytic techniques. An analyst must have a repertoire of them to apply in solving complex problems. They might include pattern analysis, trend prediction, literature assessment, and statistical analysis. A number of these techniques are presented throughout the book in the form of analysis principles. Together, they form a problem-solving process that can prevent the types of intelligence blunders discussed earlier.

A few methodologies, 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. But their use has resulted in some criticism. For instance, one author notes that

> 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.[23]

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. 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 great detail herein, as they are well covered in other texts.[24]

Sherman Kent noted that an analyst has three wishes: "To know everything. To be believed. And to exercise a positive influence on policy."[25] This book will not result in an analyst's being able to know everything—that is why we will continue to have estimates. But chapters 1–15 should help analysts to learn or refine their tradecraft of analysis, and chapters 16–19 are intended to help them toward the second and third wishes.

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, but most of the incentives in large intelligence organizations promote concealment rather than sharing of information.

- 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. A large intelligence community develops many analytic methods to deal with the variety of issues that it confronts. But the methods all work within a fundamental process: creating a model of the intelligence target (synthesis) and extracting useful information from that model (analysis). Success comes from sharing the target model with all stakeholders.

Notes

1. John Hughes-Wilson, *Military Intelligence Blunders* (New York: Carroll and Graf, 1999), 38.
2. Ibid., 102.
3. Ibid., 218.
4. Ibid., 260.
5. 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.
6. Rob Johnson, *Analytic Culture in the US Intelligence Community* (Washington, D.C.: Center for the Study of Intelligence, CIA, 2005), 70.
7. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, www.wmd.gov/report/wmd_report.pdf, overview.
8. Johnson, *Analytic Culture*, 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 get people killed.
11. Steven D. Leavitt and Stephen J. Dubner, *Freakonomics* (New York: HarperCollins, 2005), 13.
12. Johnson, *Analytic Culture*, 29.
13. National Security Archive, "The Soviet Experience in Afghanistan."
14. Ibid.
15. Amory Lovins and L. Hunter Lovins, "The Fragility of Domestic Energy," *Atlantic Monthly*, November 1983, p. 118.
16. *Report of the Commission*, March 31, 2005.
17. 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.
18. Harold P. Ford, *Estimative Intelligence* (Lanham, Md.: University Press of America, 1993), 107.
19. Johnson, *Analytic Culture*, xvii.
20. Ibid., 72.
21. CIA Center for the Study of Intelligence, "Watching the Bear: Essays on CIA's Analysis of the Soviet Union," Conference, Princeton University, March 2001, http://www.cia.gov/cis/books/watchingthebear/article08.html, 8.
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-FocusingConceptual%20Frameworks-Dec2013.pdf.
23. Ibid.
24. For two very good examples, see CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, D.C.: Author, March 2009), and Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, D.C.: CQ Press, 2011).
25. 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.