ROBERT M. CLARK

Seventh Edition

# INTELLIGENCE ANALYSIS

A Target-Centric Approach

# Intelligence Analysis

Seventh Edition

Sara Miller McCune founded SAGE Publishing in 1965 to support the dissemination of usable knowledge and educate a global community. SAGE publishes more than 1000 journals and over 800 new books each year, spanning a wide range of subject areas. Our growing selection of library products includes archives, data, case studies and video. SAGE remains majority owned by our founder and after her lifetime will become owned by a charitable trust that secures the company's continued independence.

Los Angeles | London | New Delhi | Singapore | Washington DC | Melbourne

# Intelligence Analysis

## A Target-Centric Approach

Seventh Edition

Robert M. Clark

SAGE | CQPRESS

FOR INFORMATION:

CQ Press
An Imprint of SAGE Publications, Inc.
2455 Teller Road
Thousand Oaks, California 91320
E-mail: order@sagepub.com

SAGE Publications Ltd.
1 Oliver's Yard
55 City Road
London, EC1Y 1SP
United Kingdom

SAGE Publications India Pvt. Ltd.
B 1/I 1 Mohan Cooperative Industrial Area
Mathura Road, New Delhi 110 044
India

SAGE Publications Asia-Pacific Pte. Ltd.
18 Cross Street #10-10/11/12
China Square Central
Singapore 048423

Acquisitions Editor: Christy Sadler

Editorial Assistant: Avren Keating

Production Editor: Astha Jaiswal

Copy Editor: Amy Marks

Typesetter: diacriTech

Indexer: Integra

Cover Designer: Scott Van Atta

Marketing Manager: Jennifer Haldeman

Printed in the United States of America

ISBN 9781071895283

Library of Congress Control Number: 2022911456

This book is printed on acid-free paper.

22 23 24 26 10 9 8 7 6 5 4 3 2 1

# BRIEF CONTENTS

# CONTENTS

# TABLES, FIGURES, AND BOXES

# PREFACE

The first edition of this book was published in 2003. In it, I argued that intelligence analysis should be a team effort, an inclusive process that required the participation of both collectors of raw intelligence and customers of the finished product. The aim of the *Target-Centric* approach is to replace the dated "intelligence cycle" with an interactive analyst-collector-customer process focused on the intelligence target.

This approach accomplishes three basic tasks. First, it makes it easy for customers to ask questions and for analysts to clarify them. Second, it uses the existing base of intelligence information to provide immediate responses to the customer. Third, it manages the expeditious creation of new information to answer remaining questions. The community must provide what is called "actionable intelligence"—that which is relevant to customer needs, is accepted, and is used in forming policy and in conducting operations. And above all, intelligence customers want anticipatory[1] intelligence, or answers about what will happen next. Collaboration enables such an outcome; and as this seventh edition goes to press, the US intelligence community has just produced a sterling illustration.

Analysts accurately predicted Russia's invasion of Ukraine and provided repeated warnings up to the day, on February 24, 2022. The United States and its allies took the unprecedented step of sharing the intelligence not just with each other, but with the public. They operationalized intelligence to a degree not previously seen. That action forestalled Russian plans to conduct "false flag" operations to justify the invasion. As the assault proceeded, the allies also provided tactical intelligence in near real time to Ukraine's military, allowing the Ukrainians to get inside the decision loop of Russian forces. The result was an early combat debacle that shattered long-standing myths about Russian military power. It all happened because national customers were able to publish intelligence or share it with Ukraine quickly while protecting the source.

Today, anticipatory analysis like that demonstrated in the Ukrainian conflict is the gold standard of intelligence. During the past two decades, the US and allied intelligence communities have evolved into a nimble and effective force in applying anticipatory conceptual models and methodologies to meet that standard. The result? This may be one of the most exciting and rewarding times to be in the analysis profession.

This book's primary audiences are practicing intelligence analysts, the military, and university students who are interested in entering the profession. The book is

[1] The term anticipatory has largely replaced estimative in US intelligence practice. It is defined in the introduction to part III.

written from the perspective of an all-source analyst, but it has a much broader analytic clientele. Intelligence officers who in the past were called single-source analysts (such as GEOINT and COMINT analysts) now must do all-source analysis, and the material here is relevant for them. It is intended to be of interest to all intelligence professionals and customers of intelligence, in governments, the military, and the private sector.

Intelligence practitioners can spend their entire careers in highly specialized disciplines, and many books are devoted to topics covered only briefly here. This book, rather, is a general guide, with references to lead the reader to more in-depth studies and reports on specific topics or techniques. The book offers insights that intelligence customers and analysts need to function in this new era of intelligence.

Many concepts described herein are not new. Defining the problem, assessing information gaps, forecasting and probabilistic reasoning, modeling and simulation, identifying likely decisions, presenting intelligence conclusions, and much more were captured in a 1985 CIA guide for analysts.[2] Technology has enabled advancements in them all, but the fundamentals remain.

Many examples of intelligence failures are discussed in the book, possibly leading a reader to get the impression that we experience more failures than successes. Quite the opposite is true. The events in Ukraine in 2022 represent just a few examples of many such successes. But there are reasons that most successes have not been published, leaving the failures, real and perceived, more visible. This book focuses a lens on those missteps for two reasons. First, sharing our intelligence lapses openly ensures that there will be fewer of them in the future. Second, as in any field of endeavor, we often learn more from our failures than from our successes.

## What's New?

The major change in this seventh edition is the addition of a new chapter on the emerging field of prescriptive intelligence. In addition, the advancements in the application of a target-centric approach within fusion centers merited extensive revision to chapter 6. New case studies and updated examples have been added throughout.

Some chapters have been revised to improve their use in both introductory and advanced intelligence studies courses. Parts I and II (chapters 1–14) are well suited for introductory and intermediate analysis coursework. Part I contains stand-alone chapters, in the sense that they can be introduced in any order during a course. In contrast, each chapter in part II builds on the preceding chapters, and so they should be read in order. The structure of parts I and II is designed to permit an instructor to assign analysis problems for students to use in creating an intelligence assessment as they progress through a course, drawing as necessary on the advanced concepts presented in part III.

[2] CIA, "Handbook of Problem-Solving Techniques for Intelligence Analysts," January 3, 1985.

Part III covers estimative or anticipatory intelligence and the major target-modeling approaches used by experienced analysts. It concludes with a look at the future: prescriptive intelligence. This content is accessible for all readers, but it will be of most interest to advanced students, practicing intelligence analysts, or those who simply enjoy a challenge.

A major hurdle for new analysts is not just to learn the concepts of critical thinking (which most introductory analysis courses teach) but to develop the ability to think critically about issues. To address this need, all chapters after the introduction feature a short set of critical thinking questions or exercises at the end.

# ACKNOWLEDGMENTS

I'm thankful for the efforts of my wife and partner in this effort, Abigail, whose extensive revisions made this a better book. I also thank SAGE Publishing and copy editor Amy Marks for shaping the finished product.

All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or view of the CIA or any other US government agency. Nothing in the contents should be construed as asserting or implying US government authentication of information or Agency endorsement of the author's views. This material has been reviewed by the CIA to prevent the disclosure of classified information.

Robert M. Clark

Wilmington, North Carolina

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.

# 2 INTELLIGENCE IN THE AGE OF CONTESTED NORMS AND PERSISTENT DISORDER

The violent conflicts that have erupted throughout the world in the past two decades bear little resemblance to the interstate wars of the previous millennium. These current engagements are often referred to by terms such as *hybrid wars*.[1] In 2003, one of Australia's most prolific writers on international security, Alan Dupont, characterized the change succinctly:

> *The state on state conflicts of the 20th century are being replaced by Hybrid Wars and asymmetric contests in which there is no clear-cut distinction between soldiers and civilians and between organised violence, terror, crime, and war.*[2]

Even earlier than that, in 1999, Chinese People's Liberation Army colonels Qiao Liang and Wang Xiangsui published a book titled *Unrestricted Warfare*, in which they described their vision of a new form of conflict. It was prophetic about what was to come in this century. Their main points were as follows:

> *If in the days to come mankind has no choice but to engage in war, it can no longer be carried out in the ways with which we are familiar.*
>
> *. . . The degree of destruction is by no means second to that of a war, represent(ing) semi-warfare, quasi-warfare, and sub-warfare, that is, the embryonic form of another kind of warfare.*
>
> *War which has undergone the changes of modern technology, globalization, and the market system will be launched even more in atypical forms. In other words, while we are seeing a relative reduction in military violence, at the same time we are seeing a defined increase in political, economic, and technological*[3] *violence.*
>
> *The new principles of war are no longer exclusively "using armed force to compel the enemy to submit to one's will," but rather are "using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests."*[4]

The US Joint Chiefs of Staff (JCS) developed much the same perspective on conflicts for the next two decades, albeit using different terms, which form this chapter's title. The JCS's view was explained in the 2016 publication *The Joint Force in a Contested and Disordered World*:

> Contested norms *will feature adversaries that credibly challenge the rules and agreements that define the international order.* Persistent disorder *will involve certain adversaries exploiting the inability of societies to provide functioning, stable, and legitimate governance.*[5]

Conventional wars that involve large-scale engagements (such as the first and second Persian Gulf wars) undoubtedly will continue. And great power competition shows no sign of disappearing; indeed, the events of 2022 demonstrate exactly the opposite. But much of intelligence today is about hybrid wars or unrestricted conflict, which are not conventional and which extensively involve nonstate actors. The ongoing conflicts in Syria, Iraq, and Yemen, and Boko Haram's activities in Africa are all examples. And the 2022 assault on Ukraine provides an example of both: large-scale enagagements and hybrid war that follows the model described by Qiao Liang and Wang Xiangsui. Law enforcement intelligence must deal with another type of unconventional conflict with transnational criminal enterprises. And transnational corporations must deal with types of competition that business leaders thirty years ago would not recognize—including conflicts with customers and suppliers.

The 2016 JCS publication summarized the major features of today's conflicts. Violent ideological competition will continue to focus on the subversion or overthrow of established governments. Both state and nonstate actors will continue to rely on destabilizing methods, force, or the threat of force to advance their interests against opponents. Internal political divisions, environmental stresses, and external interference will combine to disrupt and bring down governments. Cyberspace has become a major contested arena in which these conflicts take place.[6]

The strategies and tactics themselves aren't new. Unconventional warfare and subversion of existing governments date back to ancient history. When faced with superior military force, an opponent inevitably moves to what is called *asymmetric warfare* (a form of conflict that exploits dissimilarities in capabilities between two opponents). Guerrilla warfare was common in ancient China. Nomadic and migratory tribes such as the Scythians, Goths, and Huns used forms of it to fight the Persian Empire, the Roman Empire, and Alexander the Great. Similar tactics were used with success during the American Revolution and the Civil War. Niccolò Machiavelli in his sixteenth-century work *The Prince* describes all the types of conflicts prevalent today, along with advice on how a national leader should deal with them. But Machiavelli could not have envisioned the nature of today's tools, discussed in the next two sections.

## NATURE OF TWENTY-FIRST-CENTURY CONFLICT

The unique features of twenty-first-century conflicts—the ones that distinguish them from past eras—have been shaped by globalization and information technology. These two factors have increased the prevalence of networks and of nonstate actors in conflicts.

### Networks

John Arquilla and David Ronfeldt of RAND Corporation coined the term *netwar* and defined it as a form of information-related conflict, in which opponents form networks—also known as *network-centric conflict*. Specifically, Arquilla and Ronfeldt used the term to describe the "societal struggles" that make use of new technologies.[7] The technologies they discuss are available and usable anywhere, as demonstrated by the Zapatista netwar as far back as January 1994. A guerrilla-like insurgency had developed in Chiapas, Mexico, led by the Zapatista National Liberation Army. The Mexican government's repressive response caused a collection of activists associated with human-rights, indigenous-rights, and other types of nongovernmental organizations (NGOs) elsewhere to link electronically with similar groups in Mexico to press for nonviolent change. What began as a violent insurgency in an isolated region mutated into a nonviolent but disruptive social netwar that engaged the attention of activists around the world and led to both nationwide and foreign repercussions for Mexico. The Zapatista insurgents skillfully used a global media campaign to create a supporting network of NGOs and embarrass the Mexican government in a form of asymmetric attack.[8]

Nearly three decades later, in 2022, netwars were active in many regions of the world involving states, nonstate actors, and commercial entities. In the Middle East, two major protagonists headed networks in the region that have been competing for years:

- Iran was providing financial and military support to Hezbollah in Lebanon, to President Bashar Al-Assad's regime in Syria, to the Zaydi Houthis in Yemen, and to Shiite militias in Iraq. Under the banner of Shiite solidarity, Iran also provided nonmilitary aid for industrial projects, madrasas, mosques, and hospitals in Shiite regions.[9]

- Saudi Arabia, for its part, provided weaponry and funding to Sunni combatants in Syria, Iraq, and Yemen. Riyadh also deployed its military forces to support the Sunni cause in some cases. In 2011, it sent armored units into Bahrain to quell the pro-democracy rallies of the country's Shiite majority. Beginning in 2015, it intervened in Yemen to support opponents of the Zaydi Houthis in what has become a proxy war with Iran.[10]

The year 2022 was the scene of the most comprehensive netwar to date. It took the form of an extension of conventional war in Ukraine and involved cyberattacks as well as conflicting messages in social media. One of the most remarkable of these was the cyberwar launched against Russia and its supporters by a global activist group that calls itself Anonymous. Anonymous succeeded in hacking Russian government, news outlets, and corporate websites; Russian oligarchs; and Western companies that continued to do business in Russia after sanctions were imposed. Its successes included revealing personal information on 120,000 Russian soldiers fighting in Ukraine.[11]

Criminal, insurgent, and terrorist groups have their own networks that conduct economic, political, and military activities on a global scale. Their ability to access financing, advanced weaponry, and recruits extralegally makes them powerful players in international affairs—more powerful than many states, in fact. Their skill in adapting to changing environments and to threats also exceeds that of many governments.

Obviously, netwar has moved into social media, a powerful tool for gaining an advantage. The Russian operation to influence the 2016 US presidential election is well known and publicized, but netwars are being carried on continuously in social media. One author has defined these types of political netwars as

> *actions taken by governments or organized non-state actors to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts (false amplifiers) aimed at manipulating public opinion.*[12]

Networks, of course, have been used in conflicts for centuries. The American Revolution, after all, was a kind of netwar: Thirteen colonies were supported by France on one side; and Great Britain was supported by loyalists and some American Indian tribes on the other. Both world wars involved conflicting networks of states aided by guerrilla units and governments-in-exile. But the importance of networks in conflicts has increased because networks make better use of the tools of conflict discussed later in this chapter and because of the enhanced role of nonstate actors, discussed next.

## Nonstate Actors

Participants in twenty-first-century conflicts are not all governments. Many networks, as the preceding section indicates, are composed of criminal groups, commercial enterprises, and many other types of nonstate actors. The Zapatista netwar described earlier displayed the effectiveness of such actors. Some commercial enterprises, for example, engage in illicit arms traffic, support the narcotics trade, and facilitate money laundering. While states continue to be the principal brokers of power, increasingly there exists a profusion of nonstate centers of power that include unconventional and transnational organizations. These groups operate with their own rules and norms that differ markedly from the traditional rules observed by governments.[13] Intelligence is most concerned with the following major nonstate actors:

- *Insurgents.* A few examples illustrate the direction of twenty-first-century hybrid warfare in which insurgency was key: the conflict between Israel and Hezbollah in Lebanon, 2006; the emergence and expansion of Daesh (referred to in the United States as the Islamic State of Iraq and the Levant [ISIL] or the Islamic State of Iraq and Syria [ISIS]) beginning in 2011; and the Ukrainian separatist conflict that began when Russia seized Crimea in 2014. These shared several common features. The insurgents made use of sophisticated weaponry such as armor and antiarmor weapons and surface-to-air missiles. They had support from states not directly involved in the conflict—with Iran supporting Hezbollah, some Gulf states supporting Daesh, and Russia supporting Ukrainian separatists.
- *Transnational criminal enterprises.* These Mafia-like organizations engage in narcotics and human trafficking, piracy, illegal natural resources and wildlife trafficking, cybercrime, and money laundering—in the process destabilizing regions, subverting governments, and operating in failed states. The largest such entity for many years, Japan's Yamaguchi-gumi, engages in drug trafficking, gambling, and extortion. Yamaguchi-gumi's annual revenue at one point was approximately $80 billion, more than the gross domestic product of countries such as Libya and Cuba. In recent years, the Yamaguchi-gumi has fragmented and fallen into decline, but it remains one of the world's largest criminal organizations. Russian Mafia groups such as Solntsevskaya Bratva continue to thrive under Vladimir Putin's regime and have extensive international operations.
- *Individuals.* Networks must communicate to plan and execute operations, giving intelligence agencies an opportunity to discover their plots. The "lone wolf" poses a different problem. When a single person is the key player, the intent to commit a terrorist act is far more difficult to identify. Most lone-wolf terrorists are followers of radical movements—often, but not exclusively, radicalized Islamists. As a counterexample, Norwegian anti-Muslim right-wing extremist Anders Breivik killed 77 people in July 2011 during a bomb attack in Oslo followed by a shooting spree on a nearby island.

An ongoing example of netwar involving both state and nonstate actors is the one between Turkish president Recep Tayyip Erdoğan and Muslim cleric Fethullah Gülen.

## BOX 2.1 NETWAR I: ERDOĞAN VERSUS GÜLEN

During the 1980s, Turkish cleric Fethullah Gülen founded and led a powerful movement that opposed secular elements in Turkey. His supporters exercised influence in the country's political and justice systems, and the Gülen movement had expanded worldwide to include religious schools, charities, and media outlets. During this time, the Gülen movement grew into perhaps the largest Muslim network in the world. Called *Hizmet* (Turkish for "service"), it was loosely organized, with no formal structure and no official membership. Yet, it developed a following in the millions, and the funding it garnered was measured in billions of dollars.

Gülen also developed close ties with the Turkish Justice and Development Party (AKP) and its leader, Prime Minister Recep Tayyip Erdoğan. Erdoğan wielded political power; and Gülen supporters became entrenched in the civil service, police force, prosecutors' offices, and judiciary. But, in 2013, the alliance between Gülen and the Turkish government began to disintegrate. The two parted ways when Gülen criticized Erdoğan's crackdown on protesters in May of that year. Erdoğan subsequently began a campaign to purge Gülen supporters from the Turkish government.

In 2016, a Turkish military faction attempted to overthrow now-president Erdoğan's government. The coup failed; subsequently, approximately 50,000 people were reportedly arrested and 170,000 accused of complicity in the coup attempt. Those arrested or charged included many associated with the Gülen movement. President Erdoğan accused Gülen of instigating the coup and directed the closing of Gülen schools in Turkey, seizing the movement-owned newspaper *Zaman* and several companies that had ties with Gülen.

The aftermath of the coup has been a full-scale netwar between the Erdoğan government and the Gülen movement. It was still ongoing in 2021, when the Turkish government managed to have Gülen's nephew, Selahaddin Gülen, extradited from Kenya to face criminal charges. We'll revisit this case later in the chapter, after an introduction to the tools used in netwar.

Nonstate actors rely on strategies and tactics that often are not available to governments. The use of terror weapons such as improvised explosive devices (IEDs), assassinations, and public executions of captives are not options for most governments. Insurgents also use creative techniques that don't involve direct encounters with superior force and increasingly make use of the tools of conflict. The four basic types of tools are not new. What is new is the way that the tools, lethal and nonlethal, are used, including advanced technologies, and the strategies that accompany them. These are different enough from past methods that they change the game. Let's take a closer look at the four types available to nonstate actors (and to state actors as well, though the two may use the tools differently) before returning to the Erdoğan-Gülen case.

## TOOLS OF CONFLICT

In the 1960s, the US military defined four top-level levers through which a state exercises its power to influence events or deal with opponents. The military called these levers *instruments of national power*: political, military, economic, and psychosocial. Over the years, there have been several iterations of this breakdown. For example, some authors divided "psychosocial" into psychological and informational.[14] In the business world, the levers are almost the same: political, economic, environmental, and social.

Today, four such instruments are widely recognized and applied in new ways by both state and nonstate actors: diplomatic (or political), information (which replaces "psychosocial" in the 1960s definition), military, and economic, usually referred to by the acronym DIME. We'll use the DIME construct in this book. Note that the DIME instruments are identical to the "military, political, economic, and technological" forms of violence identified by colonels Qiao Liang and Wang Xiangsui.

### Diplomatic

The diplomatic (or political) tool has a long history. It nevertheless remains a powerful one for mustering the others—information, military, and economic. The most effective instrument wielded by the United States against the Soviet Union during the Cold War arguably was diplomatic: the organization of military and economic alliances aimed at thwarting Soviet expansion and limiting Soviet influence worldwide. This was the execution of the US "containment" policy.

In 2014, the United States again used diplomacy to lead a coalition with the European Union and other international partners to impose stiff sanctions on Russia for its seizure of Crimea. The United States joined an even larger alliance, including the United Nations, in imposing a series of trade and financial sanctions on North Korea from 2006 to 2018 because of its nuclear weapons and missile testing. The most dramatic such use of diplomacy, though, was the imposition of sweeping economic and political sanctions on Russia because of its 2022 Ukraine invasion. Countries that had not participated in 2014, such as Switzerland and Sweden, joined the effort. The unprecedentedly severe sanctions crippled the Russian economy.

Nonstate actors also use political tools to covertly infiltrate and subvert uncooperative or hostile governments, though usually as part of a network that includes nation-states. In the conflicts described in this chapter, each such group has some level of backing by a nation-state.

### Information

The information instrument has always had power to shape events. Propaganda has been used in conflicts for centuries. But the vehicles for delivering information have steadily expanded its reach and effectiveness. Its current form, information technology, has been a game changer in the twenty-first century, enabling more effective use of the other tools as well as being a method for mobilizing supporters, recruiting fighters, and obtaining funding.

Worldwide, both the participants in conflicts and the events they create engender extensive media attention. The international press covers all such hostilities in detail, often taking a sensational view. Leaders leverage this coverage to promote their positions and rally international support.

The internet has become the dominant vehicle for applying the information instrument. Most visible is the surface web, which is routinely used for disseminating and obtaining information, and for communication. But nonstate actors make extensive use of the *deep web*—the part not indexed (and, therefore, not searchable) by search engines. Terrorists and transnational criminal groups especially use *darknets*[15] and the *dark web*, both of which function within the deep web, to communicate clandestinely.

Cyber operations are used extensively by nonstate actors who rely on social media in both the surface web and the deep web to conduct such operations. These operations are useful for raising funds, distributing propaganda, discrediting opponents, recruiting followers, and targeting critical infrastructure or opposing leadership for the application of other instruments. Daesh became a leading example of how to use cyber operations in conflicts. It employed social media to recruit jihadists in the United States and Europe and to encourage lone-wolf attacks on military and law enforcement personnel.[16]

Cyber operations often are used to attack. They are employed to mislead and confuse opponents, shape social and political views, attack infrastructure or economies, or conduct hacking attacks on websites. In that role, they arguably could be considered as a type of military tool (the application of a different type of force). But because they are linked so closely to other information tools, offensive cyber operations are treated in this book as an information instrument.

## Military

We've seen many advances in the capabilities of military units, thanks to the application of technology. Two classes of weaponry were developed and improved over the past few decades, changing the nature of the military instrument.

One class is precision weaponry, which until recently was available only to advanced powers. Its benefit is in precisely attacking high-value targets while minimizing collateral damage. Highly accurate air-to-ground missiles, guided by laser designators, the Global Positioning System (GPS), or both, are today's tools of choice in counterterrorism operations. Increasingly, precision weapons that include surface-to-air missiles have been acquired by less advanced countries and nonstate actors.

The other class involves indiscriminate weapons, often used as instruments of terror or in a form of asymmetric warfare used against advanced military powers or hostile populations. This class includes IEDs and vehicle-borne IEDs (VBIEDs); suicide bombers; rockets launched into urban areas; and chemical, biological, nuclear, and radiation weapons.

A developing challenge is the use of the two threats combined: unmanned aerial vehicles (UAVs, or drones) that can be precisely guided to a target to deliver an IED or an incendiary, chemical, or biological weapon.[17] Drones are widely available, relatively affordable, and easily fitted with explosive devices. Their use by terrorist and insurgent groups is becoming commonplace. During 2020 and 2021, Yemen's Houthi insurgents launched a series of drone and cruise missile attacks on Saudi Arabian oil facilities. Militaries worldwide are joining the trend, as well. During early 2022, the Ukrainians used Turkey's Bayraktar drones and US "Switchblade" drones to cause havoc among invading Russian forces, in what some observers see as a major shift in the nature of combat.[18]

## Economic

International organizations and coalitions rely on sanctions and embargoes as economic instruments against states that defy international norms, using the political instrument to enforce them. Nonstate actors rely on the military instrument to acquire economic benefits—for example, through piracy, kidnappings, and hostage taking. And both state and nonstate actors rely on economic tools to conduct financial transactions that subvert the international rule of law.

The economic instrument uses the internet extensively, both for traditional financial transactions and for the informal transactions that characterize an undercover economy. Currency manipulation and international trade in illegal goods are examples:

- The hawala informal system for transferring money long has existed in the Middle East, North Africa, and India. It comprises a large network of funds brokers that functions on mutual trust. Hawala operates in parallel to but separate from international banking and financial channels. It now relies heavily on the internet for communicating the details of funds transfers.

- Since its invention in 2008, Bitcoin has become an important online payment mechanism. This virtual currency relies on peer-to-peer transactions. Although it is widely used in legitimate financial transactions, Bitcoin (along with a variety of other major cryptocurrencies such as Ethereum and Cardano) also serves those who want to avoid having their transactions tracked.

- The dark web—the clandestine side of the deep web—is a primary vehicle for online payments of all types that participants wish to conceal. Darknet markets sell drugs, software exploits, and assassination and fraud services, among others. The Silk Road case, described below, illustrates how the practice works.

## BOX 2.2 SILK ROAD

Between 2011 and 2013, Ross Ulbricht led a team that created and managed the world's largest online black market for illegal drugs. Named "Silk Road" for the ancient trade route between China and Europe, the website operated as a darknet, concealing itself and its users by relying on the Tor browser. (Tor protects the identity, location, and transactions of users by bouncing communications through a distributed network of relays run by volunteers around the world.) Silk Road handled illegal goods, mostly drugs such as heroin, methamphetamine, MDMA, and LSD, using only Bitcoin for transactions. During its nearly three years in operation, the Silk Road team collected 614,305 Bitcoin in commissions—worth approximately $80 million at the time of Ulbricht's arrest in October 2013.[19] In May 2015, Ulbricht was sentenced to a double life sentence plus forty years in prison without the possibility of parole. His appeal to the US Supreme Court unsuccessful, he turned to the information instrument, employing both traditional and social media attention. A clemency petition has obtained 500,000 signatures; however, at the close of 2021, he remained in prison.

## SYNERGY OF THE TOOLS

Many examples in this chapter involve military actions, where *military* is defined in a broad sense to mean "use of armed force." But interests of intelligence today are not strictly military. And almost all types of conflicts make use of diplomatic, economic, and information dimensions, usually applied in a synergistic fashion. The negotiations between Western powers and Iran on constraining Iran's nuclear weapons program in 2014–2015 are an example of nonmilitary conflict that encompassed each of these factors. Both sides developed political coalitions for support—with the United States, European powers, several Middle Eastern countries, and some NGOs on one side; the Iranians, Russians, and some NGOs on the other. Economic levers included trade embargoes against Iran. Iran in turn used its economic and political connections to evade sanctions to some extent. Both sides used the information instrument to rally political and social support: The Western powers focused on fears of a nuclear-armed Iran, and the Iranian government stoked anger at the United States and appealed to Iranian pride about independence from foreign pressure. Within the Middle East, the information lever was used to target social divisions, with Iran rallying Shiite Muslims to its cause, and Saudi Arabia leading the Sunni Muslims in opposition. The negotiations ended with a nuclear deal struck in 2015 between Iran and six world powers: the United States, the United Kingdom, Russia, France, China, and Germany. In 2018, President Trump announced that he was withdrawing the United States from the deal, against the objections of the European allies. During 2021, negotiations to restart the deal began, with both sides resuming their use of the tools to garner international support.

Synergy of the tools is an essential characteristic of netwars. Let's revisit the Erdoğan versus Gülen case for an example of just how that works.

### BOX 2.3 NETWAR II: ERDOĞAN VERSUS GÜLEN

The Erdoğan-Gülen netwar illustrates how the instruments of power are employed in combination.

Within Turkey, the government has made extensive use of the military instrument (primarily law enforcement) to arrest or intimidate anyone suspected of association with Gülen. Internationally, it has wielded political power—successfully pressuring governments in twenty countries to shut down Gülen movement schools, revoking passports, and using organizations such as Interpol to obtain the arrest and deportation of opposition in sixteen countries.[20] Erdogan has put continuing diplomatic pressure on the United States to extradite Gülen (who has resided in Pennsylvania since 1999). In 2017, according to a *Wall Street Journal* article, US Special Counsel Robert Mueller was investigating an alleged meeting between former White House national security adviser Michael Flynn and senior Turkish officials, during which they allegedly discussed an offer by the Turks to pay $15 million if Flynn and his son would arrange for Gülen to be deported to Turkey.[21]

One of the persons arrested after the 2016 coup attempt was Andrew Brunson, an American pastor who had lived in Turkey for years. The Turkish government claimed that Brunson was a Gülen supporter; it's more likely that he represented a bargaining chip, possibly for the extradition of Gülen. The US government had pressed Turkey since 2016 for Brunson's release. In August 2018, citing the Brunson case as a factor, the US government imposed steep tariffs on Turkish steel and aluminum—allowing Erdoğan to make use of the informational instrument, rallying Turks behind his government by claiming Turkey was a victim of economic warfare.[22] (The Turkish government released Brunson in 2018.)

The Gülen movement lacks the diplomatic and military instruments the Turkish government can wield. It is primarily left with economic and informational instruments, though it must work less visibly than its opponent. Most Gülen-linked media outlets in Turkey have been closed, but the movement continues to have a media presence elsewhere in the world. And it appears to have adequate funding to continue its operations. Unconfirmed reports suggest that the movement's 130-plus charter schools in the United States are a source of funding,[23] and the Turkish government has pushed the US government to investigate or close Gülen-affiliated schools. As a result of the ongoing political, economic, and informational conflict between Turkey and the United States, it appears that Gülen has a powerful ally in the continuing netwar.

## THE FUNCTION OF INTELLIGENCE

Twenty-first-century conflicts call for an evolving pattern of intelligence thinking, if we in the business are to provide the support that our customers need. Chapters 3–7 outline how to provide such support. As an introduction, we'll spend the remainder of this chapter focusing on the role that intelligence has always played and still must play in the age of contested norms and persistent disorder. Chapter 3 will address how the intelligence process itself has changed.

## The Nature of Intelligence

Intelligence is about *reducing uncertainty in conflict*. It does not necessarily include physical warfare because conflict can consist of any competitive or opposing action resulting from the divergence of two or more parties' ideas or interests. If competition or negotiation exists, then two or more groups are in conflict. There can be many distinct levels, ranging from friendly competition to armed combat. Also, context determines whether another party is an opponent or an ally. Parties can be allies in one situation, opponents in another.[24] For example, France and the United States are usually military allies, but they sometimes are opponents in commercial affairs.

Reducing uncertainty requires intelligence to obtain information that the opponent prefers to conceal. This definition does not exclude the use of openly available sources, such as hard-copy media (newspapers and journals) or the internet, because competent analysis of such open sources frequently reveals information that the other side wishes to hide. Indeed, intelligence in general can be thought of as the complex process of understanding meaning in available information. A typical goal of intelligence is to establish facts and then to develop precise, reliable, and valid inferences (hypotheses, estimations, conclusions, or predictions) for use in strategic decision making or operational planning.

How, then, is intelligence any different from the market research that many companies conduct or from traditional research as it is carried out in laboratories, think tanks, and academia? After all, both are intended to reduce uncertainty. The answer is that most of the methods used in intelligence are identical to those pursued in other fields, with one important distinction: In intelligence, when accurate information is not available through traditional (and less expensive) means, a wide range of specialized techniques and methods unique to the intelligence field are called into play. Academics, for example, are unlikely to have intercepted telephone communications at their disposal in conducting analysis. Nor must a lab scientist deal routinely with concealment, denial, or deception.

Because intelligence is about conflict, it supports *operations* such as military planning and combat, cyber operations, diplomatic negotiations, trade negotiations and commerce policy, and law enforcement. The primary customer is the person who will act on the information—the executive, the decision maker, the combat commander, or the law enforcement officer. Writers therefore describe intelligence as being *actionable* information. Not all actionable information is intelligence, however. A weather report is actionable, but it is not intelligence.

What distinguishes intelligence from plain news is the support for operations. Intelligence always has the purpose of supporting decisions by reducing uncertainty. The customer does (or should do) something in response to intelligence, whereas consumers typically do not do anything in response to the news—though they may do something in response to the weather report. The same information can be both intelligence and news, of course: For example, food riots in Somalia can be both if the customer must act on the information.