6 EDITION

Intelligence Analysis

A Target-Centric Approach

Robert M. Clark

Intelligence Analysis

Sixth 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

Sixth 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: Scott Greenan
Editorial Assistant: Lauren Younker
Production Editor: Tracy Buyan
Copy Editor: Amy Marks
Typesetter: Hurix Digital
Proofreader: Scott Oney
Indexer: Amy Murphy
Cover Designer: Ginkhan Siam
Marketing Manager: Jennifer Jones

Printed in the United States of America

Library of Congress Cataloging-in-Publication Data

Names: Clark, Robert M., author.

Title: Intelligence analysis: a target-centric approach / Robert M. Clark.

Description: Sixth Edition. | Washington, DC: CQ Press / SAGE, [2019] | Previous edition: 2017. | Includes bibliographical references.

Identifiers: LCCN 2019000714 | ISBN 9781544369143 (Paperback: acid-free paper)

Subjects: LCSH: Intelligence service–Methodology.
Classification: LCC JF1525.I6 C548 2019 | DDC 327.12–dc23 LC record available at https://lccn.loc.gov/2019000714

This book is printed on acid-free paper.

19 20 21 22 23 10 9 8 7 6 5 4 3 2 1

Contents

Tables, Figures, and Boxes

PART I THE PROCESS, THE PARTICIPANTS, AND THE PRODUCT

2. Intelligence in the Age of Contested Norms and Persistent Disorder

3. The Intelligence Process

6. The Analytic Network

PART II THE ANALYSIS PROCESS

8. The Intelligence Issue

9. Target Models

10. The Target Framework

11. Analyzing Existing Intelligence

12. The Information Sources: Filling Gaps

13. Denial, Deception, and Signaling

PART III ANTICIPATORY ANALYSIS AND MODELING

15. Anticipatory Analysis: Forces

16. Anticipatory Analysis: Methodology

17. Outcome Scenarios

18. Systems Modeling and Analysis

19. Relationship Modeling and Analysis

20. Geospatial Modeling and Analysis

21. Simulation Modeling

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. I had two objectives:

- To replace the dated "intelligence cycle" with an interactive analyst-collector-customer *process* focused on the intelligence target
- To promote conceptual models and methodologies to help advance anticipatory[1] analysis, that most complex of analytic endeavors

As this sixth edition goes to press, both objectives appear to be within reach. The redefined intelligence analysis process (what I call the target-centric approach) has been adopted, at least in concept, within the U.S. and other intelligence communities. And in those communities, the gold standard of intelligence analysis is now anticipatory intelligence.

The first edition was in print soon after the terrorist attack on U.S. soil of September 11, 2001, and the U.S.-led invasion of Iraq, more commonly called the Iraq War, on March 20, 2003. Those two events focused the world's attention on apparent failures of the U.S. intelligence community.

But as Stephen Marrin has pointed out, in the case of the 9/11 attack, more important are the strategic policy failures that preceded the intelligence failures.[2] And as former national intelligence officer Paul Pillar observed, the 9/11 Commission report (published in September 2004) appears to have been shaped to fit political purposes rather than to conduct an objective inquiry.[3] Arguably, *both* the 9/11 attack and the Iraqi weapons of mass destruction (WMD) debacle resulted primarily from failures in U.S. strategic policy, abetted by intelligence failures. The intelligence failures in both cases were collaborative rather than causative.

Nevertheless, the two events caused enough consternation within the United States to spawn bipartisan commissions of inquiry, resulting in the aforementioned 9/11 Commission report and the Iraqi WMD Commission report (published in March 2005). These two documents provided us with perhaps the most detailed assessments of intelligence failures ever written at the unclassified level. The reports led directly to dramatic and controversial changes in the structure of the U.S. intelligence community.

Improved intelligence, though, comes from having a better *process*, not a better structure. An effective intelligence process then will lead to an effective structure. A major contribution of the 9/11 Commission and the Iraqi WMD Commission was their focus on a failed process, specifically on that part of the process where intelligence analysts interact with their policy customers.

An intelligence process should accomplish three basic tasks. First, it should make it easy for customers to ask questions and for analysts to clarify the questions asked. Second, it should use the existing base of intelligence information to provide immediate responses to the customer. Third, it should manage the expeditious creation of new information to answer remaining questions. To do these things, intelligence must be collaborative and anticipatory: collaborative to engage *all* participants while making it easy for customers to get answers; anticipatory because intelligence customers above all else want to know what will happen next.

The *target-centric approach* to the intelligence process helps analysts and customers accomplish these three tasks by bringing together all participants in the production of sound intelligence. Though intelligence communities are organized hierarchically, the target-centric approach outlines a collaborative process for intelligence collectors, analysts, and customers to operate cohesively against increasingly complex opponents. We cannot simply provide more intelligence to customers; they already have more information than they can process, and information overload encourages intelligence failures. The community must provide what is called "actionable intelligence"—intelligence that is relevant to customer needs, is accepted, and is used in forming policy and in conducting operations. Collaboration enables such intelligence. The convergence of information technology and multimedia communications allows analysts, collectors, and their customers to interact more closely as they move from traditional hierarchies to networks—a process that had already begun to emerge before the restructuring of the U.S. intelligence community.

The second objective of the book is to clarify and refine the analysis process by drawing on existing anticipatory methodologies. These include the analytic tools used in organizational planning and problem solving, science and engineering, law, and economics. In many cases, these are tools and techniques that have endured despite dramatic changes in information technology over the past fifty years. All can be useful in making intelligence predictions, even in seemingly unrelated fields. In fact, several unifying concepts can be drawn from these disciplines and applied when creating scenarios of the future, assessing forces, and monitoring indicators.

This book's primary audiences are practicing intelligence analysts, the military, and university students who are interested in entering the profession. The book is written from the perspective of an all-source analyst, but it has a much broader analytic clientele. Intelligence officers who have in the past been called single-source analysts (such as GEOINT and COMINT analysts) now must of necessity do all-source analysis, and the material in this book is relevant for them as well.

It is also intended to be of interest to all intelligence professionals and customers of intelligence, in governments, military, and private sectors. 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 alike need in order to become more proactive in the changing world of intelligence.

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. Most major intelligence services have more analytic successes than failures. But there are reasons that successes cannot be published, leaving the failures, real and perceived, more visible. This book focuses a lens on the missteps for two reasons. First, sharing our intelligence failures openly ensures that there will be fewer of them in the future. Second, as in any field of endeavor, we probably learn more from our failures than from our successes.

What's New?

This sixth edition is a complete rewrite of the book, primarily in response to suggestions made by readers. The previous editions' wide use in academia and by government agencies and contractors has resulted in insightful recommendations, and I have attempted to incorporate those ideas throughout.

There are many new case studies and examples, but the most obvious change is in the book's organizational structure. The material has been revised for ease of 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. Part III covers estimative or anticipatory intelligence and the major target-modeling approaches used by experienced analysts. 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. New, more current examples have been added and are the basis for some of the critical thinking questions. Finally, replacing the appendix included in previous editions is a capstone case study of two U.S. national intelligence estimates (chapter 22) with a series of critical thinking questions at the conclusion. Topics for questions come from relevant chapters, so alternatively the exercise can be threaded throughout an academic course.

Acknowledgments

Many people throughout the U.S. intelligence community and academia have provided wisdom that I have incorporated. I cannot name them all, but I appreciate their help. I am especially grateful to reviewers within and outside the U.S. intelligence community who have contributed their time to improving the text. A special thanks to Mike Collier, associate professor of homeland security at Eastern Kentucky University. He pointed out to me the value of including causal modeling and graciously allowed me to include his material on the subject. And my thanks to my coauthor on two other books, William Mitchell, for his review of the fifth edition and extensive suggestions for improving it, many of which I have incorporated. Above all, I'm thankful for the efforts of my wife and partner in this effort, Abigail, whose extensive revisions made this a better book.

In addition to several anonymous reviewers, I wish to thank Chad Cogan of Tulane University and Vincent E. Henry of Long Island University, Riverhead. I also want to thank CQ Press acquisitions editor Scott Greenan, senior project editor Tracy Buyan, editorial assistant Lauren Younker, 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 U.S. government agency. Nothing in the contents should be construed as asserting or implying U.S. 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

NOTES

1. The term *anticipatory* has largely replaced *estimative* in U.S. intelligence practice. It is defined in the introduction to Part III.
2. Stephen Marrin, "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis," *Intelligence and National Security* 26, no. 2–3 (May 2011): 182–202.
3. Paul R. Pillar, *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform* (New York, NY: Columbia University Press, 2011).

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 intelligence, and the distinct types of intelligence. Chapters 1 and 2 establish the setting. Chapter 3 introduces two views of the intelligence 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 of intelligence. 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 the types of intelligence products and some cautions about the product.

CHAPTER

1 Introduction

Intelligence analysis long existed in the shadows. When intelligence 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 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, all of that has changed. The intelligence analysis discipline has emerged from the shadows in part as the result of what might be called a 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. An intelligence analysis story, in fact, 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 to this book, we often learn more from our failures than from our successes. 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 subsequent 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 notable 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. 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.[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. Relying on these assumptions, Israel's chief of military intelligence dismissed intelligence 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 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 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 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, 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 intelligence estimate on Iraq's possession of weapons of mass destruction (WMD), the inability or unwillingness of collectors and analysts to share intelligence was a recurring cause of failure.

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.[6] They did not effectively share information. 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.[7] Most governmental intelligence organizations, including the U.S. intelligence community, place more emphasis on secrecy than on effectiveness.[8] The penalty for producing poor intelligence usually is modest. The penalty for improperly handling classified information can be career-ending.[9] There are legitimate reasons not to share; the U.S. 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.[10] 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 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.[11] 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 over the past decade 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.[12] 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 cited at the beginning of this introduction, intelligence analysts or national leaders were locked into a *mindset*—a consistent thread in analytic failures. Louis Pasteur warned about that trap in his field long ago: "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. 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 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. 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.

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

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."[16] 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, considerable discussion is devoted to the vital importance of analysts being able to assess and understand their customers and their customers' 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.[17] The disadvantages of that separation became apparent, as analysis was not addressing the customer's 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 we've just covered. All intelligence analysis depends on following a process that is based on 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, conceptual frameworks sensitize analysts to the underlying assumptions in their analysis and enable them to better think through complex problems.[18]

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 avoiding failures is to *share* the model with collectors of information and customers of intelligence.

While all analysis follows a basic process, within that process and framework many analytic methodologies have been developed to deal with specific issues. In fact, studies have found that no baseline standard analytic methodology 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 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 U.S. intelligence analysts.[20]

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.[21]

There also are 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. Together, they form a problem-solving process that can prevent the types of intelligence blunders highlighted earlier.

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.*[22]

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 detail herein, as they are well covered in other texts.[23]

Sherman Kent, who is generally regarded as the father of U.S. intelligence analysis, noted that an analyst has three wishes: "To know everything. To be believed. And to exercise a positive influence on policy."[24] 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. 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: 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. John Hughes-Wilson, *Military Intelligence Blunders* (New York, NY: 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. 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.
7. Rob Johnson, *Analytic Culture in the U.S. Intelligence Community* (Washington, DC: Center for the Study of Intelligence, CIA, 2005), xvi.
8. Ibid., 11.
9. 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.
10. Steven D. Leavitt and Stephen J. Dubner, *Freakonomics* (New York, NY: HarperCollins, 2005), 13.
11. Johnson, *Analytic Culture*, 29.
12. Ibid., 70.
13. Savranskaya, "The Soviet Experience in Afghanistan."
14. Ibid.
15. Amory Lovins and L. Hunter Lovins, "The Fragility of Domestic Energy," *Atlantic Monthly*, November 1983, 118.
16. 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.
17. Harold P. Ford, *Estimative Intelligence* (Lanham, MD: University Press of America, 1993), 107.
18. 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.

19. Johnson, *Analytic Culture*, xvii.
20. Ibid., 72.
21. 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/.
22. Ibid.
23. 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).
24. 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.

CHAPTER 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 new types of conflicts 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 it they described their vision of a new form of conflict. Their book may have gotten more attention in Washington than it ever did in Beijing, but it was prophetic about what was to come in this century. Its 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 U.S. 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. But much of intelligence today is about hybrid wars or unrestricted conflict, which are not conventional and which extensively involve nonstate actors. The recent conflict in Syria/Iraq, the Afghan insurgency, the Ukraine crisis, and Boko Haram's activities in Africa all exemplify this newer type of conflict. Law enforcement must also 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 will be a major contested arena in which these conflicts will 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 that are prevalent today, along with advice on how a national leader should deal with them. But Machiavelli could not have envisioned the nature of the tools being employed today, as 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 conflicts of 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 describe the idea of conflict between networks in their discussion of the impact of new communications and information technologies on military structures, doctrines, and strategies. They 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 use 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 back in 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 had 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]

More than two decades later, in 2018, netwars were active in many regions of the world involving states, nonstate actors, and commercial entities. In the Middle East, two major protagonists headed major networks in conflicts across the region:

- 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 against the Zaydi Houthis in what has become a proxy war with Iran.[10]

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 most governments.

And netwar has moved into social media, which has become a powerful tool for gaining an advantage in conflicts. The Russian operation to influence the 2016 U.S. 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.*[11]

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 nonstate actors. They include criminal groups, commercial enterprises, and many other types of nonstate actors. The Zapatista netwar described earlier indicates the importance of nonstate 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.[12]

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 all had several features in common. 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 trafficking in natural resources and wildlife, 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 about $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 Russian Mafia groups continue to thrive under Vladimir Putin's regime and have extensive international operations.
- *Individuals.* Networks must communicate to plan and execute operations, giving intelligence an opportunity to discover their plots. The "lone wolf" poses a different problem. When a single person rather than a unit or an organization 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.

A recent example of netwar involving both state and nonstate actors that expanded dramatically in 2018 is the one between Turkish president Recep Tayyip Erdoğan and Muslim cleric Fethullah Gülen.

Nonstate actors rely on strategies and tactics that often are not available to governments. The use of terror weapons such as improvised explosive devices

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 split 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—which we'll revisit later in this chapter, after an introduction to the tools used in netwar.

(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 advanced technologies and tools of conflict. The tools themselves are not new. What is new is the way that the tools, lethal and nonlethal, are used and the strategies that accompany them. These are different enough from past methods that they change the game, often to the advantage of the nonstate actor. Let's take a closer look at some tools that are available to both state and nonstate actors—though the two may use the tools differently—before returning to the Erdoğan-Gülen case.

Tools of Conflict

In the 1960s, the U.S. 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.[13] In the business world, the levers are almost the same: political, economic, environmental, and social. The argument has been made that information technology is a fifth major instrument of national power, or of business power, on the same level as the other four. Information technology certainly is a factor (and often the critical factor) in intelligence assessments.

Four such instruments are used widely today and applied in new ways by 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, recognizing that these are also instruments of power for organized groups other than states. 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 U.S. "containment" policy.

The use of diplomacy to form networks and alliances against opponents still can be highly effective. In 2014 the United States led in the formation of a coalition with the European Union and other international partners to impose stiff sanctions on Russia for its actions in Ukraine. Beginning in 2006 and continuing into 2018, the United States joined an even larger coalition, including the United Nations, in imposing a series of trade and financial sanctions on North Korea because of its nuclear weapons and missile testing. Nonstate actors can use political tools to covertly infiltrate and subvert uncooperative or hostile governments, usually as part of a network that includes nation-states. In the conflicts described in this chapter, each group has some level of backing by a nation-state.

Information

The information instrument is old. Propaganda has been used in conflicts for centuries. But its new form, information technology, has been the game-changer in twenty-first-century conflicts, 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*[14] 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 effectively 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.[15]

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 have been developed and improved over the past few decades and now have changed the nature of the military instrument.

One class is precision weaponry, which until recently was available only to advanced powers. Its benefit derives from its use 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 weapons class includes IEDs and vehicle-borne IEDs (VBIEDs); suicide bombers; rockets launched against urban areas; and chemical, biological, nuclear, and radiation weapons.

Another challenge is developing, in the form of a combination of the two threats: unmanned aerial vehicles (UAVs, or drones) that can be precisely guided to a target and deliver an IED or an incendiary, chemical, or biological weapon.[16] Drones are widely available, relatively cheap, and easily fitted with explosive devices. Their use by terrorist and insurgent groups is becoming commonplace. During July 2018, Russia reportedly dealt with forty-five drone attacks on its Khmeimim Air Base in Syria.[17]

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) 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 sold 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.[18] In May 2015, Ulbricht was sentenced to life in prison without the possibility of parole for his role in Silk Road.

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; and 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 for its part 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.

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 a number of the instruments are employed.

On its side, the Turkish government has wielded political power—successfully pressuring governments in twenty countries to shut down Gülen movement schools, and revoking passports and using organizations such as Interpol to obtain the arrest and deportation of its Turkish opposition in sixteen countries.[19] Within Turkey, it has made extensive use of the military instrument (primarily law enforcement) to arrest or intimidate opponents. It has put continuing pressure on the United States to extradite Gülen (who has resided in Pennsylvania since 1999). In 2017, according to a *Wall Street Journal* article, U.S. 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.[20]

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 U.S. government had pressed Turkey since 2016 for Brunson's release. In August 2018, citing the Brunson case as a factor, the U.S. 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.[21] (The Turkish government released Brunson in October 2018.)

The Gülen movement lacks the diplomatic and military instruments that the Turkish government can wield. So, its response has been to rely primarily on economic and informational instruments. The movement works less visibly than its opponent, and its use of these instruments is not widely documented. Most Gülen media outlets in Turkey have been closed, but the movement continues to have an extensive 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,[22] and the Turkish government has pushed the U.S. government to investigate or close Gülen-affiliated schools. As a result of the 2018 political, economic, and informational conflict between Turkey and the United States, it appears that Gülen has (at the moment) a new and 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 intelligence business are to provide the support that our customers need. The next few chapters outline how to provide such support. As an introduction, though, we'll spend the rest of this chapter focusing on the role that intelligence has always played and still must play in dealing with conflicts 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*. Because conflict can consist of any competitive or opposing action resulting from the divergence of two or more parties' ideas or interests, it does not necessarily include physical warfare. 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.[23] For example, France and the United States are usually military allies, but they sometimes are opponents in commercial affairs.

Reducing uncertainty requires that intelligence 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 of intelligence 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. 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 acts on the information.

Intelligence can be broadly defined at the top level as being *strategic*, *operational*, or *tactical*—so long as it is recognized that the divisions among them are blurred, and all three types can potentially occur at the same time.

Strategic Intelligence

Strategic intelligence deals with long-range issues. For the military customer, strategic intelligence is produced for senior leadership. It is used to prepare contingency plans, determine what weapons systems to build, and define force structures.[24] For national customers generally, strategic intelligence is used to create national policy, monitor the international situation, and support such diverse actions as trade policymaking or national industrial policymaking. For corporations, it typically supports strategic planning, market development plans, and investment guidance.

Strategic intelligence involves much the same process in government and business. Both look at the political structure and alliances of opponents, both create biographical or leadership profiles, and both assess the opponent's technology.

Strategic intelligence is tougher to produce than tactical intelligence, which we'll discuss later. The analyst must command more sophisticated analytic techniques. The process is similar or identical to that used for tactical intelligence but usually is more complex because of the longer predictive time frame. The analyst must spend more time because there are lots of options. One has to consider many possible scenarios, and the situation can evolve in different ways; strategic intelligence, therefore, takes a long-term analytic view.

One problem is that the intelligence analyst is seldom able to put aside short-term tactical support to customers while developing a clientele having the long-term view.[25] The analyst needs a champion in the customer suite to support him or her in strategic intelligence because tactical intelligence, dealing with immediate issues, can easily consume all available resources.

The essence of strategic intelligence is best understood in terms of the methodology used in strategic planning, known as SWOT:

Strengths
Weaknesses
Opportunities
Threats

The SWOT methodology is the basis of all strategic planning, though it is not always made explicit. New techniques for strategic planning pop up from time to time, but SWOT always underlies them.

Strategic intelligence using SWOT has a long history in competitive intelligence. Businesses routinely turn to their strategic planning staff for SWOT assessments, because looking at strengths and weaknesses means looking internally. But looking at opportunities and threats means looking externally; and for that, companies rely on their competitive intelligence unit. Governmental intelligence units also look at the "OT" part of SWOT. And not just for strategic intelligence, but also for operational and tactical intelligence, as discussed in the following sections.

Operational Intelligence

Operational intelligence focuses on the capabilities and intentions of adversaries and potential adversaries. It is defined as the intelligence required for planning and execution of specific operations. The military coined the term to describe intelligence that is used primarily by combatant and subordinate joint force commanders and their component commanders. It keeps them abreast of events within their areas of responsibility and estimates when, where, and in what strength an opponent will stage and conduct campaigns and major operations.[26] But operational intelligence also is used by national-level, law enforcement, and business entities to support operational planning.

At the national level, once policy has been established, the intelligence customers have to develop operational plans to execute the policy or to carry out the strategic plan. Consider the following examples of operational plans:

- It could involve planning for diplomatic negotiations. Intelligence then must determine what the opposing negotiators want and what they will agree to.
- It could involve planning for a trade embargo. Here, intelligence must determine what sanctions are likely to be effective and what the target country might do to defeat sanctions.
- It could involve support to research and development (R&D) that will result in new weapons systems. R&D intelligence support has to be predictive, because it can take years for a development program to produce a new weapons system, and the system must be effective in that future environment.

Operational intelligence in diplomatic efforts could involve, for example, planning the negotiation of an arms reduction treaty. In law enforcement, operational intelligence is defined as intelligence that supports long-term investigations into multiple, similar targets. In this context, operational intelligence is concerned primarily with identifying, targeting, detecting, and intervening in criminal activity.[27] Operational intelligence might, for example, support planning for the takedown of an organized crime syndicate. In competitive intelligence, it might support a campaign to gain market share in a specific product line.

The SWOT method for strategic planning is useful also for operational planning, though the emphasis is different. Whereas strategic planning is more policy oriented, operational planning is focused more on threats and on opportunities that derive from opponent weaknesses. A key point to remember is that the opponent's strengths translate directly to your threats, and the opponent's weaknesses provide your side with opportunities. Intelligence has the job of identifying those strengths and weaknesses.

For the military, operational intelligence has a specific name. The U.S. Army and Air Force call it *intelligence preparation of the battlefield*. The Navy likes to use the term *intelligence preparation of the battlespace*. Whatever the name, the process involves the detailed analysis of the enemy, surface conditions (terrain or sea), and weather within a specific geographic area. It starts before the next operation and continues throughout combat operations. Its goals include understanding the adversary's forces, doctrine, tactics, and probable courses of action, together with the physical and environmental characteristics of the target area.

Intelligence preparation of the battlefield is really just a recent name for a very old technique. At the battle of Marathon in 490 B.C.E., the Greeks determined the only feasible route for a Persian attack (think of geospatial intelligence here) and stationed their forces in a narrow valley along that route to maximize the advantages of the Greek phalanx formation while taking the Persian cavalry out of the battle.

Customers prefer operational intelligence that is predictive. Analysts have to visualize or model the enemy's tactical formations, the effect of terrain and weather, and how the enemy might alter formations to adapt to those specific conditions. But predicting an opponent's future actions is difficult. You will always lack complete information because of gaps in collection capability or because of the opponent's denial and deception. The job of intelligence is, again, *to reduce uncertainty* by assessing capabilities and likely courses of action.

Military operational planning also requires identifying enemy units that are high priority to attack. Intelligence officers with special training in *targeting* usually have this role. During the targeting process, they select and prioritize targets in accordance with the military commander's guidance and objectives and the results of the intelligence preparation of the battlefield (or battlespace). Targets may be either physical targets, such as bridges and command centers, or functional targets, such as enemy command-and-control capability. Two historical examples of how the process works are the 1990–1991 coalition operations called Desert Shield/Desert Storm, and the 2006 conflict between Hezbollah and Israel in Lebanon. The two examples illustrate the difference between operational intelligence in conventional twentieth-century warfare and that of more complex twenty-first-century conflicts.

BOX 2.4 Operation Desert Shield/Desert Storm

During Operation Desert Shield and throughout the air operations of Desert Storm, U.S. Navy and Army special operations personnel and force reconnaissance Marines established a series of observation sites along the border between Kuwait and Saudi Arabia. These sites were used for continuous visual and signals intelligence (SIGINT) surveillance of Iraqi forces across the border. Information from these ground sites was combined with imagery and SIGINT collected by coalition aircraft in the theater. The process provided an intelligence picture of the locations, combat capability, and intentions of Iraqi units in Kuwait, as well as indications of the vulnerability of Iraqi forces along the Iraq-Saudi Arabian border west of Kuwait. This thorough intelligence preparation of the battlespace contributed significantly to the subsequent successful ground offensive to liberate Kuwait.[28]

Operation Desert Shield/Desert Storm represents a conventional twentieth-century conflict, both in time and in type, against an opponent who fought conventionally. It was a coalition operation, so allied forces were also customers of the intelligence that supported operational planning. Although the trend is toward such joint actions, they present several challenges that are associated with intelligence sharing, discussed later in the book.

The Lebanon case represents a twenty-first-century conflict, both in time and in type. It illustrates the challenge of conducting operational intelligence in a situation characterized by netwar, contested norms, and persistent disorder.

BOX 2.5 Lebanon War, 2006

On July 12, 2006, Hezbollah militants in Lebanon fired rockets at Israel as a diversion for an ambush on an Israeli patrol. During the ambush, Hezbollah fighters killed three Israeli soldiers and captured two. Hezbollah then demanded the release of Lebanese prisoners in Israel in exchange for the captives. Israel responded by attacking Hezbollah and Lebanese civilian targets, followed by imposing an air and naval blockade and conducting a ground invasion of Lebanon. Hezbollah in turn launched more rockets into Israel and began a campaign of guerrilla warfare in southern Lebanon.

The Israelis' operational intelligence preparation for the conflict was strikingly different from the coalition preparation for Desert Shield/Desert Storm. Israeli operational intelligence support failed in several areas. They targeted bunkers that Hezbollah had deliberately set up as decoys, missing most of the 600 concealed ammunition and weapons bunkers in the region. Their targeting of Hezbollah leaders in Beirut and their communication infrastructure also failed. Hezbollah, for its part, demonstrated a SIGINT capability that allowed it to anticipate Israeli moves and succeeded in "turning" Israeli human intelligence (HUMINT) assets in southern Lebanon to feed back misleading information to Israeli intelligence.[29]

Hezbollah fighters were well equipped with combat and communications gear, were well trained, and used tactics designed to maximize their advantages—fighting from well-fortified positions in urban areas with advanced weaponry that included antitank guided missiles. They focused on inflicting casualties on the Israeli Defense Forces (IDF) because of a perceived unwillingness of the Israelis to accept casualties. Both sides made use of the media and NGOs such as Human Rights Watch and Amnesty International to garner international support—Hezbollah pointed to Israeli attacks on civilians and the civilian infrastructure, and Israel argued that Hezbollah was using civilians as human shields. After the conflict ended with a ceasefire on August 14, 2006, both sides claimed victory. Though Israel appeared to have won in terms of relative casualties, Hezbollah emerged almost intact with an enhanced reputation for having stood up to the much more powerful IDF.

Operational intelligence to support law enforcement has its own name. It is called *intelligence-led policing*. The term originated in Great Britain. The Kent Constabulary developed the concept after experiencing substantial increases in property-related offenses during a time when they were dealing with budget cuts. The constabulary believed that only a few people were responsible for a significant percentage of burglaries and automobile theft. Their hypothesis—which subsequent events proved to be valid—was that police would have the best effect on crime by focusing on these most common offenses.[30]

Operational intelligence to support intelligence-led policing can take several forms. Analysts can anticipate crime trends so that law enforcement can take preventive measures to intervene or mitigate the impact of those crimes. Intelligence that supports, for example, planning to shut down a gang operation or a narcotics ring would be operational. As an example, to help fight terrorism and domestic extremism, the California Department of Justice examines criminal group characteristics and intervention consequences to determine which groups pose the greatest threat to the state and how best to deal with them.

Operational planning in business can take many forms, as can the nature of the intelligence to support such planning. Planning a campaign to reduce the market share of a competitor requires knowledge of the competitor's weaknesses. Negotiations with suppliers or large customers require much the same sort of knowledge that is needed to support international treaty negotiations: what the other side must have, and what it is willing to give up.

Tactical Intelligence

The military uses the term *tactical intelligence* to refer to quick-reaction intelligence that supports ongoing operations by identifying immediate opportunities and threats (SWOT, again). As was true at both the strategic and operational levels, intelligence has a well-established role at tactical levels that is spelled out in military doctrine. This form of intelligence is associated with a concept that the U.S. military calls *battlespace awareness*. Tactical intelligence is used at the front line of any conflict. It is used by field commanders for planning and conducting battles and engagements. Tactical intelligence locates and identifies the opponent's forces and weaponry, enhancing a tactical commander's ability to gain a combat advantage with maneuvers, weaponry on target, and obstacles. It allows tactical units to achieve positional advantage over their adversaries.[31]

Tactical intelligence to support the military became much more important during recent years because of weapons technology trends. Employing highly precise weaponry and operations places a premium on highly accurate data. Intelligence systems that can geolocate enemy units to within a few meters have become more central to military maneuvers. The rapidly expanding field of geospatial analysis supports such surgical operations with mapping, charting, and geodesy data that can be used for the guidance of "smart" weapons.[32]

The result, as one author notes, is that

> *much of the effort and funds expended by the Intelligence Community since the Gulf War have focused on providing direct, real-time support to forces engaged in combat by closing the "sensor-to-shooter" loop and to meeting the information needs of the senior-level commanders directing those operations. When there are American forces deployed in active military operations, as there have been on a near-continual basis since the end of the Cold War, the highest priority is now accorded to providing intelligence to support them.*[33]

The dominance of U.S. capabilities for battlespace awareness has resulted in an added task for tactical intelligence. Targets on the battlefield typically exceed the number of available sensors and weapons that can be used against them. Thus, it is important to find and attack the most important targets. So, tactical intelligence has the job of identifying the enemy forces, systems, and activities that will yield the highest payoff in terms of disrupting their operations and combat effectiveness.

Battle damage assessment (or combat damage assessment) could be considered the final stage of battlespace awareness. It includes not only physical damage assessment but also functional damage assessment. Physical damage assessment quantifies the extent of damage to a material target. An example would be imagery indicating the center span of a bridge has been destroyed, thus severing an enemy resupply line. Functional damage is about the disruption of a target's effectiveness, whether by kinetic or nonkinetic attack. For example, it would assess the effectiveness of electronic jamming or a cyber attack on enemy command-and-control capabilities. Battle damage assessment relies heavily on quick-reaction intelligence, because the commander must decide quickly what targets need to be attacked again.

Much of law enforcement intelligence also tends to be tactical in orientation. In the law enforcement world, tactical intelligence is defined as that which contributes to the success of specific investigations.[34] Tactical intelligence is driven by the need for fast response in the military and law enforcement communities. For the national customers, it's a classified form of the news; it is called current intelligence. And tactical intelligence is used every day in situations well removed from military actions and law enforcement, as the following example illustrates.

BOX 2.6 Symantec's Tactical Intelligence

A satellite photo of the Earth spins slowly on a large plasma screen, with markers indicating the sources of online threats. At rows of computer workstations, analysts monitor firewalls and other online defenses. The displays, the layout, and the security guards all evoke the image of a war room—which it is, but for a twenty-first-century conflict.

This is Symantec's war room. Here, a different type of intelligence analyst deals with junk e-mailers who are trying to stay one step ahead of filters and blacklists that block spam; of criminal hackers who constantly work to bypass bank firewalls; and of the viruses that can flow into thousands of computers worldwide in a few seconds.

Symantec maintains this control center to defend banks, Fortune 500 firms, and millions of its software users against cyber threats. It was the front line of the battle against SQL Slammer as it surged through the Internet, knocking out police and fire dispatch centers and halting freight trains; against MSBlaster, as it clogged corporate networks and forced websites offline; and in 2017 against a new wave of ransomware such as Petya and WanaCrypt0r.

(*Continued*)

(Continued)

The analysts in Symantec's war room succeed in their tactical combat because they are expert at employing the intelligence methodology discussed in the next chapter. They have *shared models* of viruses, worms, and Trojans instantly available. They model the operational patterns of North Korean groups that use ransomware such as WannaCry to track a user's keystrokes and to lift passwords and credit card numbers. They have models of the computers that are used to spread viruses. The great plasma screen itself displays a massive model of the Internet battlefront, where the beginning of new threats can be seen. Using these models and creating new ones on the fly, these tactical intelligence analysts can analyze and defeat a new virus in minutes.

Although the preceding sections discuss three distinct types of intelligence, they actually form a continuum and sometimes all three intelligence activities are going on at the same time. They also inform each other. Operational and tactical intelligence, for example, often shape strategic thinking. And, for their part, operational planners frequently rely on strategic intelligence in preparing their plans.

SUMMARY

Twenty-first-century conflicts have distinguishing features that are important for intelligence: They take a network form, and key players are often nonstate actors who operate transnationally with the support or tolerance of governments. These actors may be insurgent, terrorist, criminal, commercial, or other nongovernmental organizations—or some combination. The resulting conflicts among such networks are often called netwars or network-centric conflicts.

As a result, much of intelligence today is about hybrid wars or unrestricted conflict. Although these are not new, they present challenges because globalization and the ubiquitous Internet provide new tools for engaging in and prevailing in conflict. These tools may be thought of as dividing into four categories, known as the instruments of national (or organizational) power. The instruments are summarized in the acronym DIME: diplomatic (or political), information, military, and economic.

In current conflicts, the primary job of all intelligence continues to be *reducing uncertainty* for the customers of intelligence. Intelligence analysis must support policy, planning, and operations across the conflict spectrum. To do so, it identifies the opponents' strengths and weaknesses and the consequent opportunities and threats to the customer's interests, captured in the acronym SWOT. The type of analysis and the speed with which it must be prepared and delivered to the customer vary accordingly:

- Analysis to support strategic intelligence tends to be in-depth research focused on capabilities and plans and to consider many possible scenarios. Its time reference is long term.
- Operational intelligence is more near-term, involving support to planning for specific operations. In military usage, it has a specific name: *intelligence preparation of the battlefield* (or *battlespace*). Operational intelligence also supports planning for economic and political activities such as trade embargoes and treaty negotiations. In law enforcement, it supports intelligence-led policing to identify or anticipate crime trends.
- Tactical intelligence support tends to be rapid response, or current intelligence, to support plan execution or crisis management; it is focused on the immediate situation and on indications and warning. Again, the military gives it a specific name: *battlespace awareness*. Battle damage assessment is one phase of battlespace awareness. Much of the intelligence support to law enforcement, to business, and to countering cyber threats is tactical in nature.

CRITICAL THINKING QUESTIONS

1. Choose an existing major crime cartel, narcotrafficker, insurgent, or street gang to consider. From that group's perspective, who are your opponents? Identify the strengths and weaknesses of the opponents, and the opportunities and threats that they pose. What weapons and tools (DIME) do you have available to use against them? What types of intelligence and specific intelligence do you need to sustain your organization in the conflict? How will you obtain it?
2. Consider the same group that you analyzed in Question #1. Diagram the group's likely organizational structure or network. You will have to make assumptions about the elements of the network, deducing them from the group's operations and results. Not all members will turn up in an online search.
3. The case titled "Netwar: Erdoğan versus Gülen" has a partial list of the DIME instruments employed by each side. Identify them. From sources available to you, can you provide a more complete list of the organizations and tools used by each side in their netwar?
4. Identify three to five norms on the Internet that can be exploited (contested) by state or nonstate actors to achieve disorder.

NOTES

[1] Frank G. Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars," Potomac Institute, December 2007, http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

2. Alan Dupont, "Transformation or Stagnation? Rethinking Australia's Defence," *Australian Journal of International Affairs* 57, no. 1 (2003): 55–76.
3. In this context, *technological* refers to the use of information technology.
4. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing, China: PLA Literature and Arts Publishing House, 1999), 5.
5. U.S. Joint Chiefs of Staff, *The Joint Force in a Contested and Disordered World*, July 14, 2016, https://fas.org/man/eprint/joe2035.pdf.
6. Ibid., iii.
7. John Arquilla and David Ronfeldt, "Cyberwar Is Coming," in *Athena's **Camp**: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Washington, DC: RAND Corporation, 1997), https://www.rand.org/pubs/monograph_reports/MR880.html.
8. David Ronfeldt and Armando Martinez, "A Comment on the Zapatista 'Netwar,'" in *Athena's Camp*, 369.
9. Ben Hubbard, "Iran Out to Remake Mideast with Arab Enforcer: Hezbollah," *New York Times*, August 27, 2017, https://www.nytimes.com/2017/08/27/world/middleeast/hezbollah-iran-syria-israel-lebanon.html.
10. Mohamad Bazzi, "No End in Sight for Saudi-Iran Proxy War," *The Straits Times*, November 16, 2017, http://www.straitstimes.com/opinion/no-end-in-sight-for-saudi-iran-proxy-war.
11. Jonathan Zittrain, "'Netwar': The Unwelcome Militarization of the Internet Has Arrived," *Bulletin of the Atomic Scientists* 73, no. 5 (2017): 300–304, https://doi.org/10.1080/00963402.2017.1362907.
12. U.S. Joint Forces Command, *Commander's Handbook for Attack the Network* (Suffolk, VA: Joint Warfighting Center, 2011), http://www.dtic.mil/doctrine/doctrine/jwfc/atn_hbk.pdf.
13. David Jablonsky, "National Power," *Parameters* (Spring 1997): 34–54.
14. A darknet is a private network overlaid on the web that relies on connections between trusted peers.
15. "US Security Chief Warns of 'New Phase' in Terror Threat," *MSN News*, May 10, 2015, http://www.msn.com/en-us/news/us/us-security-chief-warns-of-new-phase-in-terror-threat/ar-BBjy1fG.
16. Robert K. Ackerman, "Unmanned Systems the New Weapon for Terrorists," *Signal*, July 1, 2017, https://www.afcea.org/content/Article-unmanned-systems-new-weapon-terrorists.
17. "Russian Airbase Attacked by Drones in Syria," CNN, August 16, 2018, https://www.cnn.com/videos/world/2018/08/16/drone-attacks-russian-forces-aleppo-syria-pleitgen-lkl-vpx.cnn.
18. Patrick Howell O'Neill, "Silk Road Founder Ross Ulbricht Sentenced to Life in Prison," *The Daily Dot*, May 29, 2015, http://www.dailydot.com/crime/ross-ulbricht-sentencing-silk-road/.
19. Nate Schenkkan, "The Remarkable Scale of Turkey's 'Global Purge,'" *Foreign Affair*s, January 29, 2018, https://www.foreignaffairs.com/articles/turkey/2018-01-29/remarkable-scale-turkeys-global-purge.
20. James V. Grimaldi, Shane Harris, and Aruna Viswanatha, "Mueller Probes Flynn's Role in Alleged Plan to Deliver Cleric to Turkey," *Wall Street Journal*, November 10, 2017, https://www.wsj.com/articles/mueller-probes-flynns-role-in-alleged-plan-to-deliver-cleric-to-turkey-1510309982.
21. Christina Maza, "Donald Trump's Fight with Turkey's Erdoğan, Explained," *Newsweek,* August 18, 2018, https://www.newsweek.com/donald-trumps-fight-turkeys-erdogan-explained-1070848.