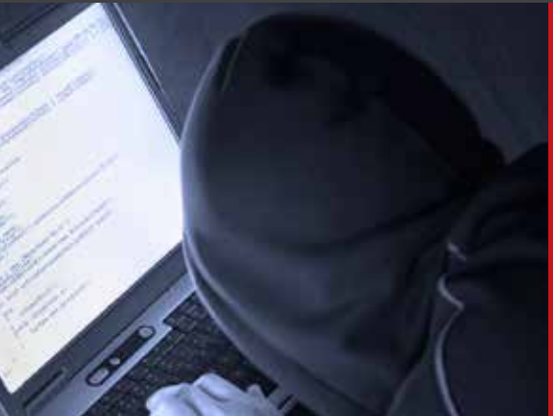
INSTRUCTOR MATERIALS

Sarah Miller Beebe
Randolph H. Pherson

SECOND EDITION

Cases in Intelligence Analysis

STRUCTURED ANALYTIC TECHNIQUES IN ACTION



Foreword by Jack Davis

Cases in Intelligence Analysis

Instructor Materials

Second Edition

To Sophia, Nora, Grant, and Nathan—with love from your mother.

To Richie and Amanda—the next generation.

Cases in Intelligence Analysis

Structured Analytic Techniques in Action

Instructor Materials

Second Edition

Sarah Miller Beebe and Randolph H. Pherson

SAGE | CQPRESS

Los Angeles | London | New Delhi
Singapore | Washington DC

Los Angeles | London | New Delhi
Singapore | Washington DC

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.
3 Church Street
#10-04 Samsung Hub
Singapore 049483

Acquisitions Editors: Sarah Calabi, Charisse Kiino
Editorial Assistant: Davia Grant
Production Editor: David. C. Felts
Typesetter: C&M Digitals (P) Ltd.
Proofreaders: Liann Lech, Annette Van Deusen
Cover Designer: Edgar Abarca
Interior Graphics Designer: Adriana M. Gonzalez
Marketing Manager: Amy Whitaker
Cover Images: ©iStockphoto.com and ©Fotolia.com

Contents

Tables, Figures, and Boxes

Note: For each chapter, the numbering of tables, figures, and boxes in these Instructor Materials continues from the numbering used in the case book for these elements.

MATRIX OF TECHNIQUES

	DECOMPOSITION AND VISUALIZATION			IDEA GENERATION					SCENARIOS AND INDICATORS				HYPOTHESIS GENERATION AND TESTING					ASSESSMENT OF CAUSE AND EFFECT			CHALLENGE ANALYSIS				DECISION SUPPORT			
	GETTING STARTED CHECKLIST	CHRONOLOGIES AND TIMELINES	MIND MAP	STRUCTURED BRAINSTORMING	STARBURSTING	MORPHOLOGICAL ANALYSIS	CLASSIC QUADRANT CRUNCHING™	FORESIGHT QUADRANT CRUNCHING™	SIMPLE SCENARIOS	MULTIPLE SCENARIOS GENERATION	INDICATORS	INDICATORS VALIDATOR™	SIMPLE HYPOTHESES	MULTIPLE HYPOTHESES GENERATOR™	QUADRANT HYPOTHESIS GENERATION	ANALYSIS OF COMPETING HYPOTHESES	DECEPTION DETECTION	KEY ASSUMPTIONS CHECK	RED HAT ANALYSIS	OUTSIDE-IN THINKING	PREMORTEM ANALYSIS	STRUCTURED SELF-CRITIQUE	WHAT IF? ANALYSIS	DEVIL'S ADVOCACY	DECISION MATRIX	FORCE FIELD ANALYSIS	PROS-CONS-FAULTS-AND-FIXES	STRENGTHS, WEAKNESSES, OPPORTUNITIES, THREATS
1. Who Poisoned Karinna Moskalenko?				❖	♦													❖			♦	♦						
2. The Anthrax Killer		♦		❖														❖			♦	♦						
3. Cyber H_2O	♦																	♦						♦				
4. Is Wen Ho Lee a Spy?																	♦	❖			♦	♦				♦		
5. Jousting with Cuba over Radio Marti		♦													♦	♦	♦											
6. The Road to Tarin Kowt																		♦						♦				♦
7. Who Murdered Jonathan Luna?		♦		❖									♦	♦		♦												
8. The Assassination of Benazir Bhutto		♦	♦													♦												
9. Death in the Southwest				♦	♦									♦		♦		♦										
10. The Atlanta Olympics Bombing														♦				♦									♦	
11. The DC Sniper							♦							♦				♦										
12. Colombia's FARC Attacks the US Homeland				♦						♦	♦	♦							♦									
13. Understanding Revolutionary Organization November 17				❖				♦			❖		♦										♦					
14. Defending Mumbai from Terrorist Attack				♦			♦				♦	♦						❖	♦									
15. Iranian Meddling in Bahrain				♦	♦	♦					♦																	
16. Shades of Orange in Ukraine				♦					♦											♦								
17. Violence Erupts in Belgrade				❖																					♦	♦	♦	

♦ The technique is featured in the case.

❖ *The technique is used implicitly in the case.*

Foreword to the Second Edition

Jack Davis, CIA Trailblazer

Some fifty years ago, Sherman Kent, legendary Chairman of the Board of National Estimates, sent an early advocate of structured analysis to make his case to a new but well-regarded member of his Estimates staff—Jack Davis.

I listened, with feigned interest, as the advocate spelled out the virtues of externalizing and evaluating the assumptions supporting key judgments of assessments. To put it directly, I saw no need to change the way I did analysis.

I rather abruptly terminated the meeting by averring, "There is no piece of paper big enough to hold all the thoughts influencing my predictions of future developments in [the countries I work on]." A response that while not helpful was not unreasonable at a time when computers had not yet replaced typewriters and my ego had not yet been tempered by several avoidable misjudgments.

It took some twenty years for me fully to appreciate and vigorously promote the analytic benefits of structured analysis, especially the insurance provided against the hazards of judgments based solely on internalized critical thinking, unstructured peer debate, and subjective boss review.

Several factors abetted the growing influence within the Intelligence Community (IC) of what was first called *Alternative Analysis* and is now called *Structured Analytic Techniques* (SATs).

- A string of highly publicized intelligence failures set off calls for changes in the conduct of analysis that gave advocates of structured analysis a foot in the door.
- A small but influential cadre of intelligence professionals began teaching and preaching about the mental, bureaucratic, and political obstacles to sound analysis spelled out with authority by Robert Jervis in the foreword to the first and present editions of *Cases in Intelligence Analysis.*
- Leading students of analytic methodology, including prominently the two authors of this book, developed, tested, and refined through case studies an impressive array of SATs to address said obstacles.

These personal observations serve as a preface to what I see as the valuable contributions to the practice of analysis of the second edition of Cases in Intelligence Analysis: Structured Analytic Techniques in Action. SATs are not "silver bullets" that automatically improve the assessment at hand and simultaneously enhance the critical thinking of the responsible analyst(s). The well-tested procedures followed in the book hold promise of achieving both goals.

- The cases range in challenge from reducing uncertainty on data-rich issues by structured organization of what is known (e.g., *chronologies*), to reducing uncertainty on data-poor issues by structured assessments of multiple plausible outcomes *(e.g., Scenarios Analysis*).
- The case texts start with stating the nature of analytic challenges, the essence of likely correctives, cost-benefit expectations from structuring, per se, and only then the effectiveness of selected SATs.
- Each case has a list of recommended substantive readings, a reminder to participants that expert knowledge serves to facilitate effective execution of structured analysis.
- The focus of learning is on sound analytic process—for example, changing the lens for viewing the case issue—rather than on coming up with the correct answer.
- In the same vein, the book shows the perils of overconfidence and heavy reliance on existing paradigms as well as the rewards of doubting and challenging the conventional wisdom.

For these and other reasons the book serves well potential and practicing analysts not only in intelligence but in all

fields of endeavor where the charge is, in effect, managing substantive uncertainty to serve clients charged with decision making and action taking.

A brief assessment of the book's potential value for one such group:

> As in the 1960s, veteran analysts assigned to craft the most important ("can't fail") assessments out of respect for their substantive expertise and critical thinking skills tend to resist intrusion of formal structuring. Some analysts see SATs as unnecessary if not also disruptive. Managers may temper this resistance by raising from their perch former President Ronald Reagan's standard of *Trust but Verify.* SATs that expert analysts can employ as self-insurance against unchallenged judgments and confidence levels include *Pre-Mortem Analysis;* and when analysts disagree, *Team A-B Analysis.*

I believe that combining the best of substantive expertise and critical thinking with the best of structured analysis provides the best protection against avoidable analytic shortfalls. *Cases in Intelligence Analysis* provides the wherewithal for helping IC analysts move toward that goal.

Preface

There's an old anecdote about a tourist who stops a New Yorker on the street and asks, "How do you get to Carnegie Hall?" The New Yorker replies, "Practice, practice, practice." The humor in the anecdote highlights an important truth: the great musicians who play at Carnegie Hall have a lot of innate talent, but none of them got there without a lot of practice.

Really great analysts have a lot of innate talent too. Whether in government, academia, or business, analysts are usually curious, question-asking puzzle solvers who have deep expertise in their subject matter. Not surprisingly, they like to be right, and they frequently are. And yet, the Iraq WMD Commission Report shows that analysts can be wrong. Analytic failures often are attributed to a range of cognitive factors that are an unavoidable part of being human, such as faulty memory, misperception, and a range of biases. Sometimes the consequences are unremarkable. Other times, the consequences are devastating. Structured analysis gives analysts a variety of techniques they can use to mitigate these cognitive challenges and potentially avoid failures, *if* analysts know when and how best to apply them. This book is designed to give analysts practice using structured analytic techniques.

Improving one's cognitive processes by using the techniques discussed in this book can be challenging but also rewarding. The techniques themselves are not that complicated, but they can push us out of our intuitive and comfortable—but not always reliable—thought processes. They make us think differently in order to generate new ideas, consider alternative outcomes, troubleshoot our own work, and collaborate more effectively.

This process is like starting a fitness regimen for the brain. At the beginning, your muscles burn a little. But over time and with repetition, you become stronger, and the improvements you see in yourself can be remarkable. Becoming a better thinker, just like becoming a better athlete, requires practice. We challenge you to feel the burn.

AUDIENCE

This book is for anyone who wants to explore new ways of thinking more deeply and thoroughly. It is primarily intended to help up-and-coming analysts in colleges and universities, as well as intelligence professionals, learn techniques that can make them better analysts throughout their careers. But this book is just as salient for seasoned intelligence veterans who are looking for ways to brush up on skills—or even learn new ones. The cases also are intended for teams of analysts who want to rehearse and refine their collaboration skills so that when real-life situations arise, they are prepared to rise to the challenge together.

CONTENT AND DESIGN

We chose the case study format because it provides an opportunity to practice the techniques with real-life contemporary issues. It is also a proven teaching method in many disciplines. We chose subject matter that is relatively recent—usually from within the past decade—and that comprises a mix of better- and lesser-known issues. In all cases, we strove to produce compelling and historically accurate portrayals of events; however, for learning purposes, we have tailored the content of the cases to focus on key learning objectives. For example, we end many of the cases without revealing the full outcome. Several cases, such as "Who Murdered Jonathan Luna?," have no known outcome. But whether or not the outcome is known, we urge students to judge their performance on the merits of their analytic process. Like mathematics, just arriving at a numerical value or "correct" outcome is not enough; we need to show our work. The value of the cases lies in the process itself and in learning how to replicate it when real-life analytic challenges arise.

The seventeen cases and analytic exercises in this book help prepare analysts to deal with the authentic problems and real-life situations they encounter every day. Taken as a whole, the seventeen cases walk through a broad array of

issues such as how to identify mindsets, mitigate biases, challenge assumptions, think expansively and creatively, develop and test multiple hypotheses, create plausible scenarios, identify indicators of change, validate those indicators, frame a decision-making process, and troubleshoot analytic judgments—all of which reinforce the main elements of critical thinking that are so important for successful analysis. Individually, each chapter employs a consistent organization that models a robust analytic process by presenting the key questions in the case, a compelling and well-illustrated narrative, and carefully chosen recommended readings. Each also includes question-based analytic exercises that challenge students to employ structured analytic techniques and to explicate the value added by employing structured techniques.

INSTRUCTOR RESOURCES

As instructors ourselves, we understand how important it is to provide truly turnkey instructor resources. The *Instructor Materials* that accompany this book are free to all readers of this book as a downloadable .pdf, and graphics from both the case book and the *Instructor Materials* are available as free, downloadable .jpeg and PowerPoint slides. We have classroom-tested each case study and applied what we have learned to enhance the *Instructor Materials* and better anticipate the instructor's needs. We believe they are just as useful to working analysts and students seeking to learn how best to apply the techniques. Just like the cases themselves, the *Instructor Materials* employ a consistent organization across all cases that puts the case and the analytic challenges in context, offers step-by-step solutions for each exercise, and provides detailed conclusions and key takeaways to enhance classroom discussion.

ACKNOWLEDGMENTS

Both authors thank Flannery Becker, Ray Converse, Claudia Peña Crossland, Mary O'Sullivan, James Steiner, and Roy Sullivan for their substantial contributions to the book. Both authors are grateful to many other individuals who helped review, test, and otherwise improve the cases, including Nigah Ajaj, Todd Bacastow, Milton Bearden, George Beebe, Mark T. Clark, Eric Dahl, Jack Davis, Matthew Degn, John Evans, Roger George, Joseph Gordon, Thomas Graham, Richards J. Heuer Jr., Georgia Holmer, Daryl Johnson, Laura Lenz, Austin Long, Frank Marsh, Richard Miles, Gregory Moore, Polly Nayak, Rudolph Perina, Marilyn Peterson, Kathy Pherson, Richard Pherson, Mark Polyak, Libby Sass, Marilyn Scott, Raymond Sontag, Leah Tarbell, Greg Treverton, Marc Warburton, and Phil Williams, as well as students of Great Plains National Security Consortium, James Madison University, Mercyhurst College, the University of Mississippi, Pennsylvania State University, and the University of Pittsburgh.

DISCLAIMER

All statements of fact, opinion, or analysis expressed in this book are those of the authors and do not reflect the official positions of the Office of the Director of National Intelligence (ODNI), the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI), or any other US government agency. Nothing in the contents should be construed as asserting or implying US government authentication of information or agency endorsement of the authors' views. The materials in the book have been reviewed by the ODNI, FBI, and CIA only to prevent the disclosure of classified material.

About the Authors

Sarah Miller Beebe began thinking about a book of cases during her career as an analyst and manager at the Central Intelligence Agency. A variety of broadening experiences, including an assignment as director for Russia on the National Security Council staff and a position as a national counterintelligence officer at the Office of the National Counterintelligence Executive, drove home the need for rigorous and effective approaches to intelligence analysis. It became apparent to her that cases could not only teach important analytic lessons surrounding historical events but also give analysts experience using a question-based thinking approach underpinned by practical techniques to improve their analyses. Now, as owner of Ascendant Analytics, she helps organizations apply such techniques against their specific analytic problems.

Randolph H. Pherson has spearheaded teaching and developing analytic techniques and critical thinking skills in the Intelligence Community. He is the author of the *Handbook of Analytic Tools and Techniques* and has coauthored *Structured Analytic Techniques for Intelligence Analysis* with Richards J. Heuer Jr., *Critical Thinking for Strategic Intelligence* with Katherine Hibbs Pherson, and the *Analytic Writing Guide* with Louis M. Kaiser. Throughout his twenty-eight-year career at the Central Intelligence Agency, where he last served as national intelligence officer for Latin America, he was an avid supporter of ways to instill more rigor in the analytic process. As president of Pherson Associates, LLC since 2003 and chief executive officer of Globalytica, LLC since 2009, he has been a vigorous proponent of a case-based approach to analytic instruction.

Together, Beebe and Pherson have developed and tested new analytic tools and techniques, created interactive analytic tradecraft courses, and facilitated analytic projects. In their work as analytic coaches, facilitators, and instructors, they have found the case approach to be an invaluable teaching tool. This second edition of case studies is their most recent collaboration and one that they hope will help analysts of all types improve both the quality and impact of their work.

Introduction

For the past two decades, a quiet movement has been gathering momentum to transform the ways in which intelligence analysis is practiced. Prior to this movement, analysts generally approached their tradecraft as a somewhat mysterious exercise that used their expert judgment and inherent critical thinking skills. Although some analysts produced solid reports, this traditional approach was vulnerable to a large number of common cognitive pitfalls, including unexamined assumptions, confirmation bias, and deeply ingrained mindsets that increased the chances of missed calls and mistaken forecasts.[1] Without a means of describing these invisible mental processes to others, instruction in analysis was difficult, and objective assessments of what worked and what did not work were nearly impossible. Moreover, this traditional approach tended to make analysis an individual process rather than a group activity; when conclusions were reached through internal processes that were essentially intuitive, groups of analysts could not approach problems on a common basis, and consumers of analysis could not discern how judgments had been reached. Absent systematic methods for making the analytic process transparent, problems that required collaboration across substantive disciplines and geographic regions were particularly prone to failure.

The desire for change has been propelled by a growing awareness that analytic performance has too often fallen short. Former Central Intelligence Agency (CIA) Deputy Directors of Intelligence Robert Gates and Doug MacEachin did much to spark this awareness within the Intelligence Community during the 1980s and 1990s, criticizing what they regarded as "flabby" thinking and insisting that CIA analysts employ evidence and argumentation in much more rigorous and systematic ways. To address these problems, Gates focused on raising the quality of analytic reviews, and MacEachin established a set of standard corporate practices for analytic tradecraft, which were disseminated and taught to CIA analysts.[2] Subsequent investigations into the failure to anticipate India's 1998 nuclear test, the surprise terrorist attacks of 11 September 2001 in the United States, and the erroneous judgments about Iraq's possession of weapons of mass destruction brought the need for analytic improvements into broader public view.

But simply realizing that improvements in analysis were needed was not sufficient to produce effective change. An understanding of the exact nature of the analytic problems, as well as a clear sense of how to address them, was required. Richards J. Heuer Jr., a longtime veteran of the CIA, provided the theoretical underpinnings for a new approach to analysis in his pioneering work *Psychology of Intelligence Analysis.*[3] In this, Heuer drew upon the work of leading cognitive psychologists to explain why the human brain constructs mental models to deal with inherent uncertainty, tends to perceive information that is consistent with its beliefs more vividly than it sees contradictory data, and is often unconscious of key assumptions that underpin its judgments. Heuer argued that these problems could best be overcome by increasing the use of tools and techniques that structure information, challenge assumptions, and explore alternative interpretations. These techniques have since come to be known collectively as structured analytic techniques, or SATs. He developed one of the earliest techniques, called Analysis of Competing Hypotheses, to address problems of deception in intelligence analysis. It now is being used throughout the community to address a variety of other analytic problems as well, helping to counter the natural tendency toward confirmation bias.[4]

Since the pioneering efforts of Heuer to understand and address common cognitive pitfalls and analytic pathologies, considerable progress has been made in developing a variety of new SATs and defining the ways they may be used. In 2011, Heuer joined one of the authors of this volume, Randolph H. Pherson, in publishing the most comprehensive work on this subject to date, *Structured Analytic Techniques for Intelligence Analysis*.[5] The book describes how structured analysis compares to other analytic methods, including expert judgment and quantitative methods, and provides a taxonomy of eight families of SATs and detailed descriptions of some fifty-five techniques. By including an in-depth discussion of how each technique can be used in collaborative team projects and a vision for how the techniques can be successfully integrated into analysis done in the intelligence, law enforcement, and business communities, Heuer and Pherson challenged analysts from all disciplines to harness the techniques to produce more rigorous and informative analysis.

WHY A BOOK OF CASES?

The books published by Heuer and Pherson have helped analysts become familiar with the range of available structured analytic techniques and their purposes, but little work has been done to provide analysts with practical exercises for mastering the use of SATs. This book is designed to fill that gap. As such, it is best regarded as a companion to both *Psychology of Intelligence Analysis* and *Structured Analytic Techniques for Intelligence Analysis*. The cases in this book—vivid, contemporary issues coupled with value-added analytic exercises—are meant to bridge the worlds of theory and practice and bring analysis to life. They compel readers to put themselves in the shoes of analysts grappling with very real and difficult challenges. Readers will encounter all the complexities, uncertainties, and ambiguities that attend real-life analytic problems and, in some cases, the pressures of policy decisions that hang in the balance.

We have chosen a case study approach for several reasons. First, the technique has proved an effective teaching tool in a wide variety of disciplines, fostering interactive learning and shifting the emphasis from instructor-centric to student-centric activity while usually sparking interest in issues previously unfamiliar to students.[6] The use of the case study approach also allows students to tackle problems on either an individual or a group basis, facilitating insights into the strengths and weaknesses of various approaches to independent and collaborative analysis. Although the seventeen cases in this book are used to illustrate how structured analysis can aid the analytic process, they also can be used to catalyze broader discussions about current issues, such as foreign policy decision making, international relations, law enforcement, homeland security, and many other topics covered in the book. It is through these types of practical exercises and discussions that analysts learn to put problems in context and develop and execute clear and effective analytic frameworks.

The cases cover recent events and include a mix of functional and regional issues from across the world. We strive to present compelling and historically accurate portrayals of events—albeit tailored for learning purposes—to demonstrate how SATs can be applied in the fast-breaking and gritty world of real-life events and policy decisions. To discourage students from "gaming" their analysis, however, we end many of the cases without revealing the full outcome in the main text, and several—such as "Who Murdered Jonathan Luna?"—have no known outcome. But whether or not the outcome is known, the purpose of the exercises is not simply to arrive at the "correct" judgment or forecast contained in the *Instructor Materials* or to make the analysis mirror the actual outcome. As with exercises in mathematics, arriving at the proper numerical value or outcome does not demonstrate mastery; that can only be demonstrated by showing the math that led one to the proper outcome. The value of the cases lies in learning the analytic processes themselves and how to apply them to real-life problems.

ORDER AND ORGANIZATION

The order of the cases roughly mirrors the hierarchy of problems that analysts face when assuming responsibility for a new portfolio or account. Typically, when starting a new assignment, analysts are asked to become familiar with past analytic reports and judgments on the topic. When done well, such a process will uncover preexisting mindsets and expose unsupported assumptions. The first cases in the book—"Who Poisoned Karinna Moskalenko?," "The Anthrax Killer," "Cyber H_2O," "Jousting with Cuba over Radio Marti," "Is Wen Ho Lee a Spy?", "The Road to Tarin Kowt," and "Who Murdered Jonathan

Luna?"—are designed to teach SATs that challenge prevailing mindsets and develop alternative explanations for events.

As analysts gain more familiarity with the issues for which they are responsible, they often encounter new developments for which no line of analysis has been developed. In such circumstances, analysts require techniques for developing and testing new hypotheses and for visualizing the data in creative and thought-provoking ways. "The Assassination of Benazir Bhutto," "Death in the Southwest," "The Atlanta Olympics Bombing," and "The DC Sniper" are designed with these goals in mind.

Finally, as analysts master their subjects, they are asked to tackle problem sets that are arguably the most difficult analytic challenges: understanding the perceptions and plans of foreign adversaries and forecasting uncertain future developments shaped by dynamic sets of drivers. In "Colombia's FARC Attacks the US Homeland," "Understanding Revolutionary Organization 17 November," and "Defending Mumbai from Terrorist Attack," students put themselves in the shoes of the adversary and develop a range of plausible future outcomes, while in "Iranian Meddling in Bahrain" and "Shades of Orange in Ukraine" students not only develop scenarios but also actively consider a range of future outcomes and specific indicators that a particular outcome is emerging. "Violence Erupts in Belgrade" rounds out the cases by placing students in a direct decision support role in which they must not only provide assessments about the forces and factors that will drive events but also develop a decision framework and troubleshoot their analysis.

Each of our case studies employs a consistent internal organization that guides the student through an analytic process. We begin each case study by listing several overarching *Key Questions.* These questions are designed as general reading guides as well as small-group discussion questions. The questions are followed by the *Case Narrative,* which tells the story of the case. This is followed by a *Recommended Readings* section. The final section, *Structured Analytic Techniques in Action,* presents focused intelligence questions and exercises to guide the student through the use of several structured analytic techniques and toward self-identification of the value added by SAT-aided analysis. The turnkey *Instructor Materials,* which are available to analysts, students, and instructors via download, put the learning points for the cases in context, present detailed explanations of how to successfully apply the techniques, and provide case conclusions and additional key takeaways that may be used in instruction.

TECHNIQUE CHOICE

The techniques are matched to the analytic tasks in each case. For example, in "Who Poisoned Karinna Moskalenko?," there are many unanswered questions that require the kind of divergent and imaginative thinking that Starbursting can prompt. In "Violence Erupts in Belgrade," Force Field Analysis helps the analyst make a judgment about the prospect of additional violence—an analytic judgment that will shape decisions about what to do to protect the US Embassy. Each case includes at least three technique-driven exercises, and each exercise begins with a discussion of how the technique can be used by analysts to tackle the kind of problem presented in the exercise. Space constraints preclude the inclusion of all techniques that might be applicable for each case; we chose those that we felt were most salient and illustrative. For example, nearly two-thirds of the cases implicitly or explicitly include a Key Assumptions Check or Structured Brainstorming, but these core techniques could easily be applied to all the cases. Overall, we strove to include a variety of SATs throughout the book that are representative of each of the eight families of techniques. To help orient readers, we have included a secondary, matrixed table of contents that details the cases and the full complement of techniques that each utilizes.

HOW CAN THESE CASES BEST FACILITATE LEARNING?

Whether students are working alone or in small groups, the cases are most effective when students and instructors view them as opportunities to test and practice new ways of thinking that can help them break through the cognitive biases and mindsets that are at the core of so many analytic failures. Viewed this way, the techniques are a means by which analysts can practice robust analytic approaches, not an end in and of themselves. Our goal was to give analysts a fun and effective way to hone their cognitive skills. We hope we have hit the mark, and we welcome feedback on the cases and the techniques as well as suggestions for their refinement and further development.

NOTES

1. See Rob Johnston, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2005), http://www.fas.org/irp/cia/product/analytic.pdf, 22–23. "What tends to occur is that the analyst looks for current data that confirms the existing organizational opinion or the opinion that seems most probable and, consequently, is easiest to support. . . . This tendency to search for confirmatory data is not necessarily a conscious choice; rather, it is the result of accepting an existing set of hypotheses, developing a mental model based on previous corporate products, and then trying to augment that model with current data in order to support the existing hypotheses."

2. See Jack Davis, "Introduction: Improving Intelligence Analysis at CIA; Dick Heuer's Contribution to Intelligence Analysis," in *Psychology of Intelligence Analysis,* ed. Richards J. Heuer Jr. (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1999, and reprinted in 2007 by Pherson Associates, LLC, Reston, VA, http://www.pherson.org), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf, xv–xix.

3. Heuer, ed., *Psychology of Intelligence Analysis.*

4. Richards J. Heuer Jr., "The Evolution of Structured Analytic Techniques," presentation to the National Academy of Science, National Research Council Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security, Washington, DC, December 8, 2009, http://www7.nationalacademies.org/bbcss/DNI_Heuer_Text.pdf.

5. Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, 2nd ed. (Washington, DC: CQ Press, 2015).

6. See Richard Grant, "A Claim for the Case Method in the Teaching of Geography," *Journal of Geography in Higher Education* 21, no. 2 (1997): 171–85; and P. K. Raju and Chetan S. Sankar, "Teaching Real-World Issues through Case Studies," *Journal of Engineering Education* 88, no. 4 (1999): 501-8.

Table 1.3 ▶ Case Snapshot: Who Poisoned Karinna Moskalenko?

Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Premortem Analysis	p. 240	Challenge Analysis
Structured Self-Critique	p. 245	Challenge Analysis
Starbursting	p. 113	Idea Generation

1 Who Poisoned Karinna Moskalenko?
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

TECHNIQUE 1: PREMORTEM ANALYSIS AND STRUCTURED SELF-CRITIQUE

This case has been written to approximate the information environment that analysts confronted in thinking about this case as it unfolded in 2008. To produce sound analysis, students must consciously go beyond the mental framework established by the media coverage and known history that surrounded the case. The exercise is aimed at pushing the student to challenge the existing mindset that prevailed at the time and to question the information presented in the media coverage.

The Karinna Moskalenko case study details the challenges posed by quickly moving events punctuated by anomalous evidence, ingrained mindsets, misleading reports, and subconsciously held biases. As students begin their analysis of this case, the court of public opinion has already spoken; Western press coverage has pointed its finger at Moscow even as it has raised and then dismissed out of hand the possibility that it could "perhaps . . . [be] an unfortunate accident."[1]

Task 1.

Conduct a Premortem Analysis and Structured Self-Critique[2] of the reigning view in the case study that "Karinna Moskalenko is the latest victim in a series of alleged Russian attacks on Kremlin critics."

Step 1: Imagine that a period of time has passed since you published your analysis that contains the reigning view just stated. You suddenly learn from an unimpeachable source that the judgment was wrong. Then imagine what could have caused the analysis to be wrong.

The first two steps in the Premortem Analysis are right-brain-led, creative brainstorming. This process asks analysts to imagine a future in which they have been proved wrong and work backward to try to identify the possible causes. In essence, they are identifying the weak links in their analysis in order to avoid these potential pitfalls prior to publishing the analysis. Most analysts are more left brained than right brained, which often makes imagination techniques like brainstorming challenging. However, when coupled with the systematic, left-brained checklist that comprises the second half of the Premortem Analysis, brainstorming can be the first step toward identifying sometimes fatal analytic flaws. It is important to encourage students to be as creative as possible when brainstorming, keeping all ideas in play.

In this case, a brainstorming session might prompt students to consider the following:

- New evidence comes to light that suggests someone other than the Russians is behind the poisoning (e.g., her husband, her children, an acquaintance, a colleague at work, or a case of mistaken identity).
- The toxicology reports were faked. She isn't ill.
- The mercury was accidentally placed in the vehicle (e.g., by her kids, the former owner of the vehicle, or someone else).

Step 2: Use a brainstorming technique to identify alternative hypotheses for how the poisoning could have occurred. Keep track of these hypotheses.

In this case, students might identify a number of alternative perpetrators of the crime. They could include the following:

- Karinna Moskalenko's husband.
- Moskalenko herself, who staged the poisoning with or without the assistance of her husband to put the Russian government on the defensive.
- A jealous work colleague.
- An acquaintance not connected to her legal work.
- Someone connected to a previous or pending case.
- An accident or fluke.

The alternatives should not include scenarios that contradict known facts in the case. Instructors may advise students that facts such as the presence of mercury in the car and that Moskalenko and her family are truly suffering from symptoms of mercury poisoning may be accepted as accurate for the purposes of the case study. As a result, any alternative hypothesis that the Moskalenko family poisoning is a hoax or that the mercury is not present would be discarded.

Step 3: Identify key assumptions underlying the consensus view. Could any of these be unsubstantiated? Do some assumptions need caveats? If some are not valid, how much could this affect the analysis?

The most important aspect of this step is the conversation it produces about the effect of assumption on the analysts' confidence level in the mainline judgment itself.

In this case, when assumptions are explicated in this manner, it becomes apparent that the key assumptions are unsupported by evidence. This lack of evidence suggests that analysts should be prepared to track down additional information, consider alternative explanations, and potentially add a caveat to or revise the mainline judgment.

Some key assumptions and notional assessments are listed in Table 1.4.

Step 4: Review the critical evidence that provides the foundation for the argument. Is the analysis based on any critical item of information? On a particular stream of reporting? If any of this evidence or the source of the reporting turned out to be incorrect, how much would this affect the analysis?

The Moskalenko case is short on hard evidence. Students should note this dearth, as well as the fact that the direct evidence in this case is based on two main sources: French police and Karinna Moskalenko's comments to the press.

Table 1.4 ▶ Key Assumptions in the Karinna Moskalenko Case

Key Assumption	Assessment
Moskalenko was a target of the Russians because of her work as a human rights lawyer.	Unsupported. There is no evidence that the Russians targeted her.
The Russians are the perpetrators because they have intentionally poisoned their enemies in the past.	Unsupported. This is a non sequitur. There is no evidence of Russian involvement.
This was intentional poisoning.	Unsupported. There is no evidence of intent; there are other possible explanations.

Other "evidence" is really historical information, speculation on the part of Moskalenko's friends and colleagues, and conclusions based on inference.

Step 5: Is there any contradictory or anomalous information? Was any information overlooked that is inconsistent with the lead hypothesis?

The key pieces of "hard evidence" in the case are the mercury found in Moskalenko's car and the press reports confirming that she suffered from mercury poisoning. Even these hard facts, however, are anomalous when examined more closely. Other information, such as the discrepancy between press headlines and actual substance of their reports, is contradictory. A notional analysis is presented in Table 1.5.

Table 1.5 ▶ Evidence Assessment in the Karinna Moskalenko Case

Evidence	Assessment
Mercury found in car	Anomalous. Why use mercury when in the past the Russians have allegedly used highly effective techniques? Mercury used in this manner is not effective. It requires specific conditions over time to poison someone.
Moskalenko's illness	Anomalous. Causing illness is an ineffective scare tactic if being used by the Russians to thwart her participation in the trial. To wit, she must get sick and know how and why at precisely the right time in order to prevent her travel. She fell ill Tuesday and went to the police two days after her husband found the mercury.
Headline versus facts	Contradictory. The press headlines read poison "fell" Moskalenko, but the French Police are cited as "cautious about the poison claim."

Step 6: Is there a potential for deception? Does anyone have motive, opportunity, and means to deceive you?

In this case there is no evidence that the Russians were intentionally trying to deceive. Moskalenko's statements to the press—and various press analyses—that the Russians are the perpetrators of the poisoning, however, could easily mislead an analyst. Although technically no deception was present because no one deliberately tried to promote a falsehood, it is useful to explore the deception question because it can prompt a discussion of whether one should take at face value what is being reported in the press and what Moskalenko is saying publicly. In this case, the judgment that the perpetrators were most likely Russian—fueled by Moskalenko herself—is a key and unsupported assumption. Assumptions masquerading as facts can reinforce preexisting mindsets and bias the analysis of other information relevant to a case. Both Moskalenko and journalists may have had motives for their allegations of Russian involvement; their motives, however, are not relevant to the question of whether there is independent evidence to substantiate the claims.

Step 7: Is there an absence of evidence, and does it influence the key judgment? (See Table 1.6)

Step 8: Have you considered the presence of common analytic pitfalls such as analytic mindsets, confirmation bias, "satisficing," premature closure, anchoring, and historical analogy? (See Table 1.7)

Step 9: Based on the answers to the themes of inquiry outlined, list the potential deficiencies in the argument in order of potential impact on the analysis.

Analysts should recognize that there are potential deficiencies in most elements of the Premortem Analysis of this case, including the following:

- Unsupported assumptions.
- Absence of evidence.
- Contradictory information.
- Presence of analytic pitfalls.

Analytic Value Added: As a result of analysis, would you retain, add a caveat to, or dismiss the mainline judgment, and why? Students should seek to dismiss the mainline judgment that the Russians poisoned Moskalenko because of the unsupported statements by the press and Moskalenko herself, and the likelihood that analytic pitfalls biased the judgment. They should cite the gaps in their information base as well as the potential for other,

Table 1.6 ▶ Absence of Evidence Assessment in the Karinna Moskalenko Case

Absence of Evidence	Assessment
No physical evidence linking the crime to the Russians	There could be another perpetrator or possible hypothesis (e.g., someone other than the Russians, accidental poisoning, self-inflicted poisoning, someone she knows who is unconnected to this case or her work).
No other sources of information other than Moskalenko's statements, the mercury found in the car, and the laboratory reports confirming that she has mercury poisoning	The dearth of information should alert us to the need for more information and at the very least affect our confidence level in our assessment pending additional, corroborative information. We should prepare collection requirements and indicate the presence of these gaps in our analysis.

Table 1.7 ▶ Common Analytic Pitfalls

Pitfall	Definition
Analytic mindset	A fixed view or attitude that ignores new data inconsistent with that view or attitude.
Anchoring	The tendency to rely too heavily on one trait or piece of information when making decisions.
Confirmation bias	The tendency to favor information that confirms one's preconceptions or hypotheses, independently of whether they are true.
Historical analogy	Using past events as a model to explain current events or to predict future trends.
Mirror imaging	Assuming that the subject of the analysis would act in the same way as the analyst.
Premature closure	Coming to a conclusion too quickly based on initial and incomplete information.
Satisficing	Generating a quick response that satisfies all stakeholders associated with the issue.

plausible alternative hypotheses. More information is needed about family dynamics, any history of marital strains, how the mercury was distributed in the car, and any potential adversaries of Moskalenko other than the Russian government.

Task 2.

Rewrite the lead judgment of the case so that it reflects any changes you would incorporate as a result of the Premortem Analysis.

Important elements that students should use to revise the judgment include these:

- While Moscow has a long history of targeting its opponents, the involvement of the Russian government in this case is unclear at this time.
- We lack direct evidence that would link the Russian government to the poisoning or that proves this was an intentional poisoning.
- If this is an intentional poisoning, there are a range of possible suspects, including the Russian government, professional associates, or even family members.
- Finally, hypotheses attributing the poisoning to an accident cannot be ruled out.

TECHNIQUE 2: STARBURSTING

Using Starbursting to brainstorm a robust list of questions about a topic can help analysts explore the same question from many different angles. It is particularly useful in this case because there preexists a firm mindset and a fairly uncontested assessment of the cause and perpetrator of the alleged poisoning.

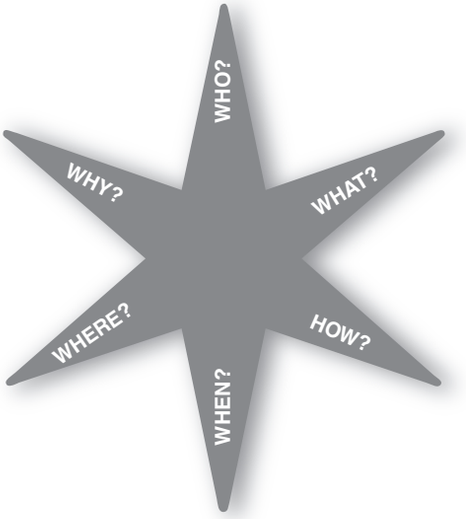
In addition, the process of drawing a Starburst diagram forces analysts to array the questions graphically around the star rather than simply list the questions. Doing so presents the analysts with a blank canvas to fill with as many questions as possible. As a result, it stimulates discussion about each point of the star and makes it more difficult for analysts to dismiss or overlook one or more angles.

Task 3.

Starburst the case "Who Poisoned Karinna Moskalenko?"

Step 1: Use the template in Figure 1.3 or draw a six-pointed star and write one of the following words at each point of the star: *Who? What? How? When? Where? Why?*

Figure 1.3 ▶ Starbursting the Karinna Moskalenko Case



Step 2: Start the brainstorming session, using one of the words at a time to generate questions about the topic. Do not try to answer the questions as they are identified; just focus on generating as many questions as possible.

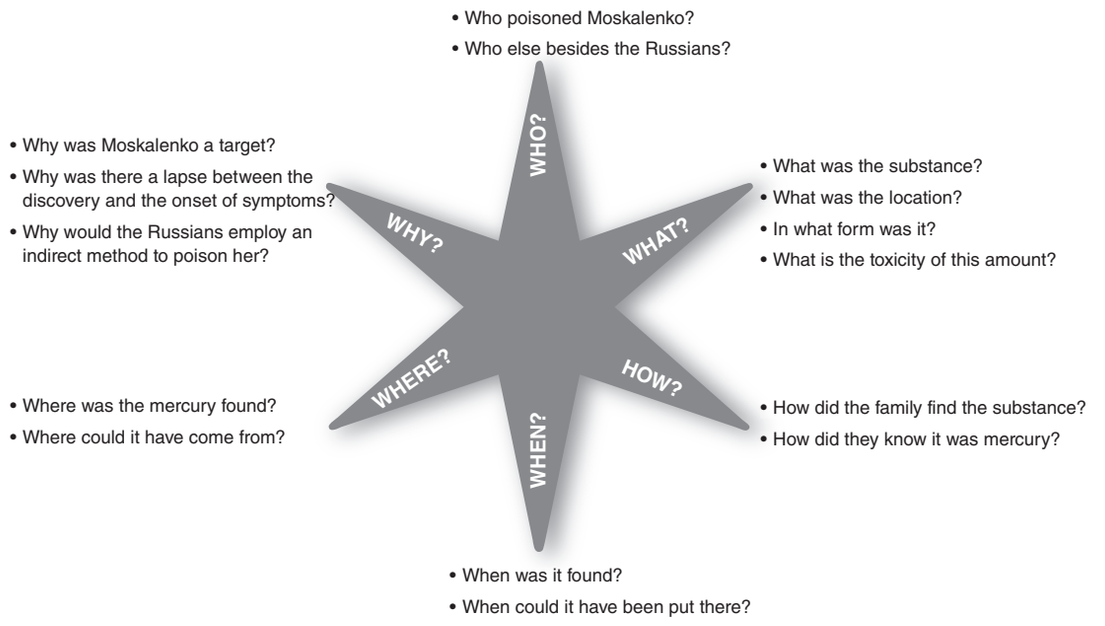
Students should be able to develop at least two to four questions per "point" in the star, as reflected in the notional Figure 1.4.

Step 3: After generating questions that start with each of the six words, the group should either prioritize the questions to be answered or sort the questions into logical categories.

Depending on the specific questions they develop, students may choose to categorize the questions on the basis of a known factor, such as supporting evidence. For instance, they could form three groups of questions: one group for questions that have evidence to support the answer, another for which there is only indirect evidence or assumptions, and another for which there is no supporting evidence at all. Alternatively, students could prioritize the questions on the basis of "known unknowns," or gaps they seek to fill.

Analytic Value Added: **As a result of your analysis, which questions or categories deserve further investigation?**

Figure 1.4 ▶ Starbursting the Karinna Moskalenko Case



Analysts could focus their assessment on those questions for which there is the least information or for which there are alternative explanations. In this case, these might include the following:

- Who else besides the Russians could be interested in poisoning Moskalenko?
- Where else could the mercury have come from?
- When could the mercury have been placed in the car?
- Why was there a lapse between the discovery of the mercury and the onset of symptoms?

This process raises the overall issue that there is no direct evidence to answer the Starburst questions for many of the key points on the star, including Who? Where? When? and Why? This should cause analysts to reassess their confidence in the overall assessment that the Russians poisoned Moskalenko with mercury because of her work as a human rights lawyer.

CONCLUSION

On 22 October 2008, only eight days after the case broke in the news media and ten days after Moskalenko and her husband discovered mercury in their car, media outlets reported that Karinna Moskalenko's poisoning was accidental.[3] The *New York Times* reported that "French investigators have concluded that the mercury found in the car of a prominent Russian human rights lawyer had been accidentally spilled from a thermometer that had been broken in the car before the lawyer bought the vehicle."[4] The assistant prosecutor in the case said that the amount of mercury in the car was not toxic and that the amount of mercury in Moskalenko's blood was "insignificant."[5] He added that mercury must be ingested or injected to be toxic.

KEY TAKEAWAYS

- Avoid a rush to judgment, even if what is happening seems obvious. Slow down the momentum in a crisis situation by always asking why a judgment could be incorrect.
- Ensure that the line of analysis is underpinned by a strong evidentiary base. Track down key gaps to avoid potentially catastrophic analytic vulnerabilities.
- Always be alert to the analytic trap of "satisficing," especially when under pressure to confirm a popular viewpoint or generate an analysis rapidly.

NOTES

1. "More Poison: Another Prominent Adversary of Vladimir Putin Is Mysteriously Exposed to Toxins [editorial]," *Washington Post*, October 22, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/10/21/AR2008102102342.html.

2. The steps as outlined in this case combine the processes for a Premortem Analysis and Structured Self-Critique. This combination is particularly helpful in cases that require analysts to think broadly, imaginatively, and exhaustively about how they might have been wrong. The Premortem Analysis taps the creative brainstorming process, and the Structured Self-Critique provides a step-by-step assessment of each analytic element. To aid students' learning process, the questions in this case have already been narrowed from the fuller set of Structured Self-Critique questions found in Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, 2nd ed. (Washington, DC: CQ Press, 2015).

3. Cyrille Louis, "L'avocate de Politkovskaïa n'aurait pas été empoisonnée [Attorney for Politkovskaya was not poisoned]," Le Figaro (France), October 22, 2008, http://www.lefigaro.fr/actualite-france/2008/10/22/01016–20081022ARTFIG00605-l-avocate-de-politkovskaia-n-aurait-pas-ete-empoisonnee-.php.

4. Alan Cowell, "France: Mercury in Lawyer's Car Is Ruled Accidental," *New York Times,* October 27, 2008, http://www.nytimes.com/2008/10/28/world/europe/28briefs-MERCURYINLAW_BRF.html.

5. Mark Ames, "Editorial Malpractice," *Nation,* December 10, 2008, http://www.thenationa.com/article/editorial-malpractice.

Table 2.1 ▶ Case Snapshot: The Anthrax Killer

Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Chronologies and Timelines	p. 56	Decomposition and Visualization
Premortem Analysis	p. 240	Challenge Analysis
Structured Self-Critique	p. 245	Challenge Analysis

2 The Anthrax Killer
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

In the following exercises, students put themselves in the shoes of an FBI analyst who must unravel how events in the anthrax case unfolded, present the information to a senior policy maker in a succinct and effective format, and troubleshoot the judgment that Steven Hatfill is most likely the anthrax killer prior to the announcement that he is the FBI's person of interest.

Analysts are often called upon to support government task force investigations in which the fast pace of events, scrutiny by high-level officials, and sheer quantity of information can be overwhelming. In the face of this kind of challenge, Chronologies frame the problem and bring order to the jumble of data points, helping analysts identify assumptions and gaps that form the case. Combined with Timelines, this ordering puts key facts and events in context so that individual analysts can easily track large amounts of data and multiperson task forces can maintain a common understanding of developments, day or night. Timelines and Chronologies can also be the basis for tailored products or graphics such as Maps that can be used to bring senior officials up to speed efficiently and effectively. The Premortem Analysis and Structured Self-Critique help analysts avoid a rush to judgment and illuminate important areas for further consideration by challenging assumptions, identifying biases, and closely examining the evidentiary base.

TECHNIQUES 1, 2, & 3: CHRONOLOGY, TIMELINE, AND MAP

Chronologies are a simple but useful tool that helps order events sequentially; display the information graphically; and identify possible gaps, anomalies, and correlations. The technique pulls the analyst out of the evidentiary weeds to view a data set from a more strategic vantage point. A Chronology places events or actions in the order in which they occurred. A Timeline is a visual depiction of those events, showing both the time of events and the time between events. Chronologies can be paired with Timeline and mapping software to create geospatial products that display multiple layers of information such as time, location, and multiple parallel events. The geographic scope and many details of this case make a Chronology, Timeline, and Map particularly useful in understanding how the case unfolded both temporally and spatially.

In the case narrative, students pick up the case on 15 October, well after the anthrax letters are sent. By creating the Chronology, the analyst develops a deeper understanding of each relevant event or piece of data. The Timeline, in turn, illustrates different temporal aspects of the case. In the following exercise, the key is to correlate the timing of the onset of illness with the letters themselves. By using the Timeline, it becomes apparent that the timing of the onset of illness overlapped significantly in New York, New Jersey, and Florida, which corresponded with the first mailing, while a separate grouping of New Jersey and Washington, D.C., cases emerges around the time of the second mailing. Also, the cutaneous cases emerged more rapidly after known exposure than the inhalation cases, which is consistent with the clinical descriptions provided by the Centers for Disease Control. The use of these techniques also highlights the importance of arranging the data by date of information, not the date of acquisition or the date of reporting. For example, the anthrax cases are tracked by date of illness onset or by date

that treatment was sought, not by the date the case was reported in the press. In fact, the FBI used a similar chronology to illustrate this point in the official Amerithrax Investigative Summary, noting, "the evidence supports the conclusions that the mail attacks occurred on two separate occasions."[1]

Task 1.

Create a Chronology of the anthrax attacks and investigation.

Step 1: Identify the relevant information from the case narrative with the date and order in which it occurred.

Step 2: Review the Chronology by asking the following questions:

- What does the timing of the appearance of symptoms tell me about when the letters were mailed?
- Could there be any other letters than the four in the government's possession?
- What additional information should we seek?
- Are there any anomalies in the timing of events?

Task 2.

Create a Timeline of the victims of the attacks based on geographic location.

Step 1: Identify the relevant information about the victims from the Chronology with the date and order in which the events occurred. Consider how best to array the data along the Timeline. Can any of the information be categorized?

Table 2.3 ▶ Chronology of the Anthrax Attacks

Date	Event
18 September 2001	Hamilton Township postal worker Richard Morgano scratches his arm while fixing a jammed machine.
19 September 2001	Robert Stevens handles a letter with "white talc."
21 September 2001	New York Post employee Johanna Huden notices a bump on her finger that later turns out to be cutaneous anthrax.
25 September 2001	Erin O'Connor handles a threatening letter addressed to NBC correspondent Tom Brokaw.
26 September 2001	Hamilton Township postal worker Richard Morgano presents with cutaneous anthrax.
28 September 2001	Casey Chamberlain, an assistant to Tom Brokaw, develops cutaneous anthrax.
28 September 2001	Hamilton Township postal worker Teresa Heller develops cutaneous anthrax.
29 September 2001	Seven-month-old child of ABC employee develops cutaneous anthrax.
1 October 2001	Ernesto Blanco falls ill in Boca Raton, FL and is diagnosed with inhalation anthrax.
1 October 2001	Erin O'Connor develops cutaneous anthrax and seeks medical attention.
1 October 2001	Seven-month-old admitted to hospital for cutaneous anthrax.
1 October 2001	Assistant to CBS News Anchor Dan Rather, Claire Fletcher develops cutaneous anthrax.
2 October 2001	Robert Stevens is hospitalized in Boca Raton, FL.
5 October 2001	Robert Stevens dies of inhalation anthrax.
8 October 2001	The FBI begins a criminal investigation into the anthrax cases. Forty agents search the American Media, Inc. building where Blanco and Stevens worked.
9 October 2001	At Hamilton Township mail center, a machine jams and a colleague of Norma Wallace shoots compressed air into the machine, sending dust particles into the air.
14 October 2001	Hamilton Township postal worker Patrick O'Donnell develops symptoms of acute cutaneous anthrax.
15 October 2001	Bret Wincup and Grant Leslie open a letter addressed to Senator Daschle and white powder pours out.
15 October 2001	The white powder in the Daschle letter is identified as purified anthrax.
15 October 2001	Hamilton Township postal worker Jyotsna Patel develops inhalation anthrax.
16 October 2001	Washington, DC Brentwood postal worker Leroy Richmond develops inhalation anthrax.
16 October 2001	An anonymous Washington, DC Brentwood postal worker called "George Fairfax" in the press develops inhalation anthrax.

Table 2.3 ▶ *(Continued)*

Date	Event
16 October 2001	Washington, DC Brentwood postal worker Thomas Morris, Jr. develops inhalation anthrax.
16 October 2001	Washington, DC Brentwood postal worker Joseph Curseen develops inhalation anthrax.
17 October 2001	Ernesto Blanco is released from the hospital.
17 October 2001	Hamilton Township postal center accountant Linda Burch develops cutaneous anthrax.
18 October 2001	The Centers for Disease Control confirms that the strains of anthrax in the Daschle and Brokaw letters match, as do the handwriting in the letters. Also in October, Northern Arizona University microbiologist Dr. Paul Keim pinpoints the strain as Ames, a strain developed in US government labs. The CDC confirms the find.
19 October 2001	Hamilton Township postal worker Norma Wallace is diagnosed with inhalation anthrax.
19 October 2001	An unnamed New York Post mailroom worker develops cutaneous anthrax.
21 October 2001	Hamilton Township postal worker Patrick O'Donnell is released from the hospital.
21 October 2001	Washington, DC Brentwood postal worker Thomas Morris, Jr. dies from inhalation anthrax.
22 October 2001	Washington, DC Brentwood postal worker Joseph Curseen dies of inhalation anthrax.
22 October 2001	State Department Mail Center Employee David Hose develops inhalation anthrax.
23 October 2001	New York Post employee Mark Cunningham develops cutaneous anthrax after going through old mail postmarked in September.
23 October 2001	Hamilton Township postal worker Jyotsna Patel is released from the hospital.
25 October 2001	Manhattan Eye, Ear and Throat Hospital stockroom attendant Kathy Nguyen develops inhalation anthrax.
31 October 2001	Manhattan Eye, Ear and Throat Hospital stockroom attendant Kathy Nguyen dies of inhalation anthrax.
9 November 2001	FBI Press Briefing provides linguistic and behavior assessment of a potential anthrax killer and asks for the public's help.
14 November 2001	Ottilie Lundren, a 94-year-old CT woman, develops inhalation anthrax.
15 November 2001	Investigators find an anthrax-laced letter to Senator Leahy in a bag of quarantined mail that was postmarked 9 October.
21 November 2001	Ottilie Lundren dies of inhalation anthrax.
June 2002	FBI releases information that radiocarbon dating indicates the spores used in the attacks were made within the last two years.
June 2002	FBI drains pond near Ft. Detrick in search of anthrax evidence.
25 June 2002	Investigators search Hatfill's apartment.
July 2002	FBI profile of the anthrax killer leaks to the press.
August 2002	Investigators pinpoint a mailbox in Princeton, NJ from which the anthrax letters were sent.
1 August 2002	Investigators search Hatfill's apartment and trash bins.
6 August 2002	Attorney General John Ashcroft names Hatfill a "person of interest."
11 August 2002	Investigators search Hatfill's apartment again.

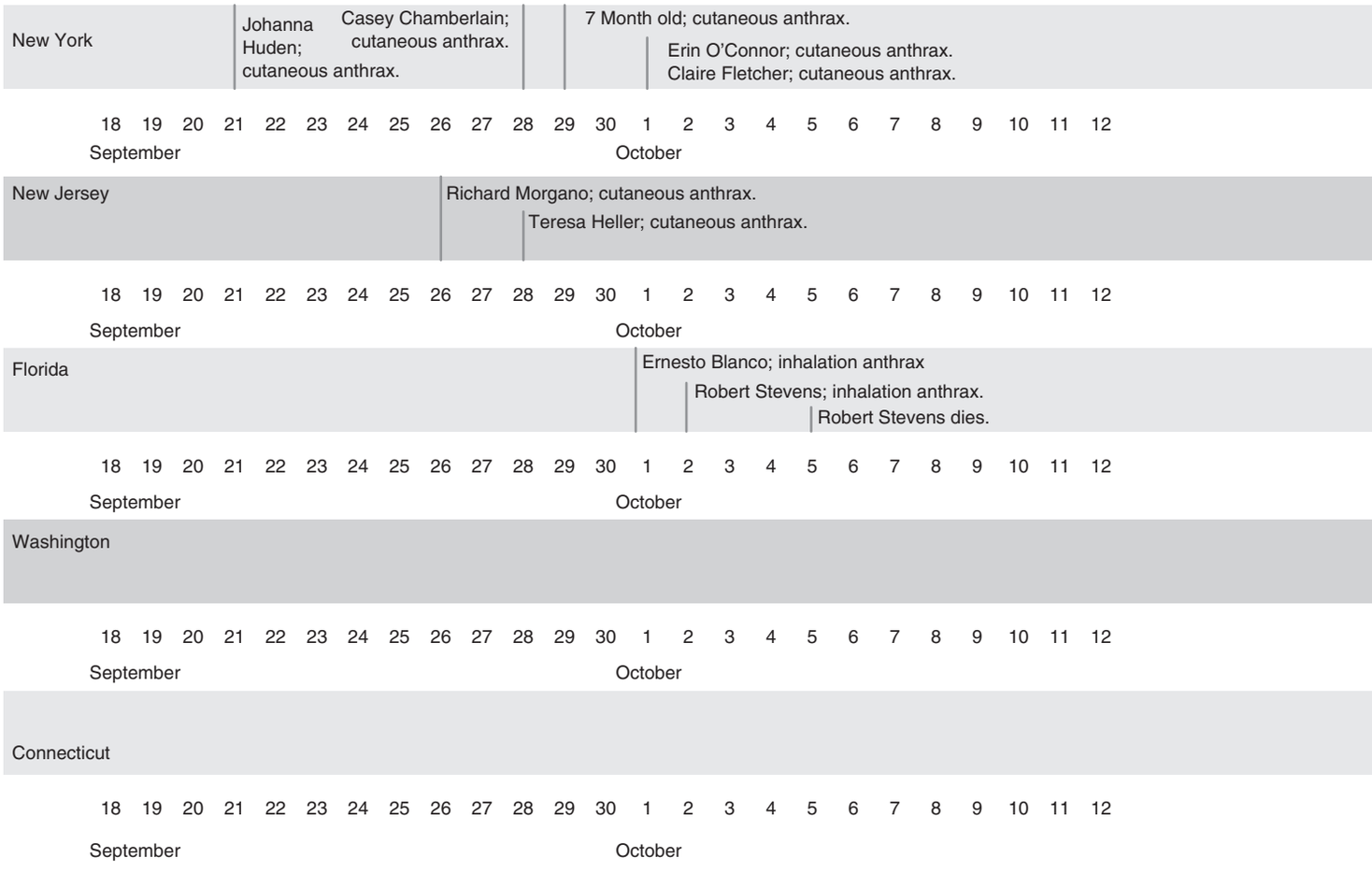
Step 2: Review the timeline by asking the following questions:

- Do any of the events appear to occur too rapidly or too slowly to have reasonably occurred in the order or timing suggested by the data (e.g., the letters and their postmarks)?
- Are there any underlying assumptions about the evidence that merit attention?
- Does the case study contain any anomalous data or information that could be viewed as an outlier? What should be done about it?

Task 3.

Create an annotated Map of the letters and twenty-two anthrax cases based on your Chronology. Visually display the information on a Map so that it could be used as a graphic for a briefing with a high-level official.

Figure 2.1 ▶ Example of a Victim Timeline in the Anthrax Case



Anthrax cases are listed by the victim's name, anthrax type, and illness onset date. Deaths are listed separately.

Students may elect to use another scheme to represent the locations and timing of the attacks. Their performance should be judged on the accuracy and effectiveness of their chosen approach, not the degree to which they reproduce the map used in this example.

Step 1: Use publicly available software of your choosing to create a Map of the area.

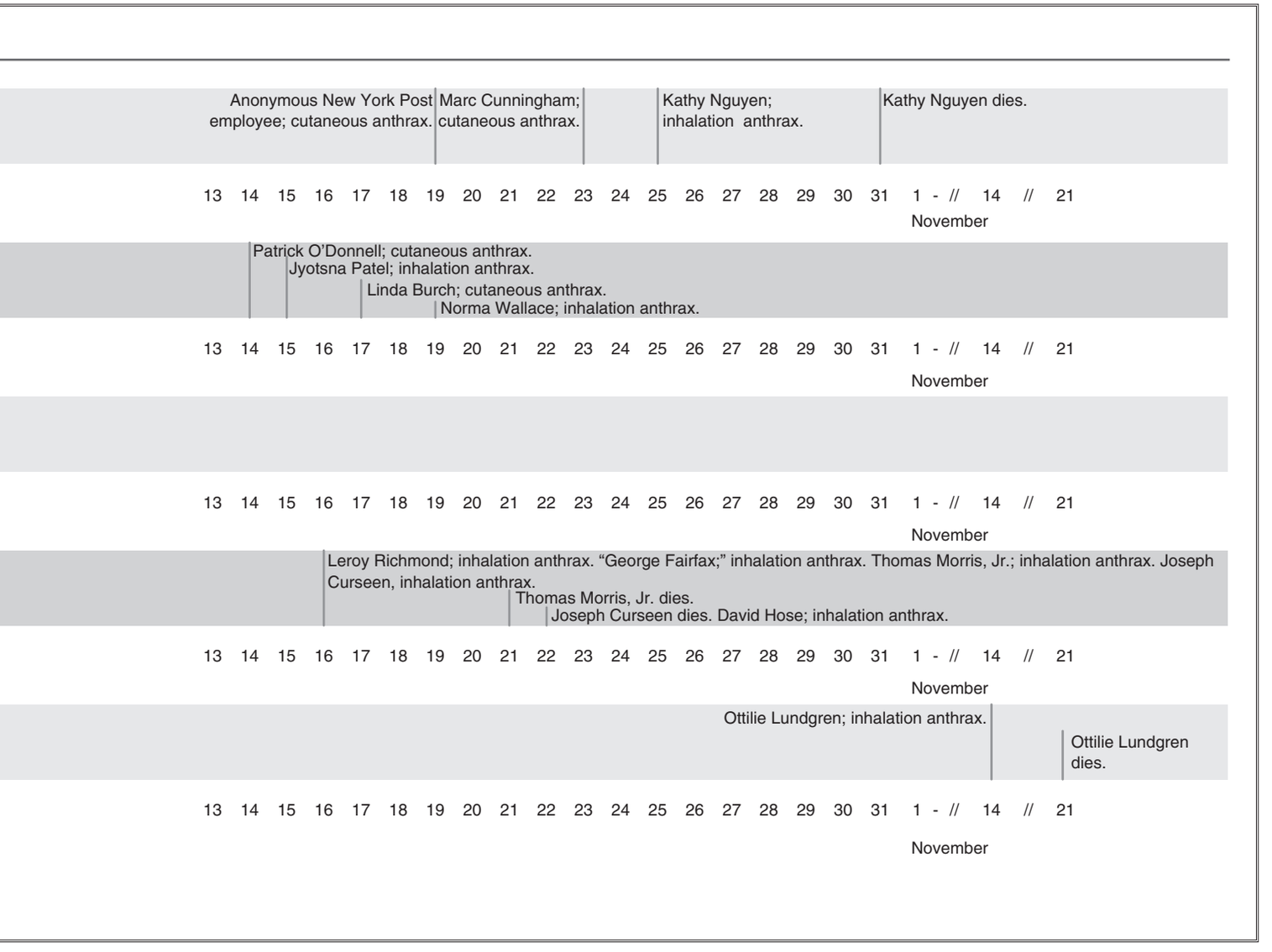
Step 2: Overlay the route (location, case type, prognosis).

Step 3: Annotate the Map with appropriate times and locations presented in the case.

Analytic Value Added: What do the locations and sequence of events tell you? What additional information should you seek? Do you agree with investigators' findings that the four letters to date and a fifth unknown letter are most likely responsible for the anthrax cases to date? The cases in New York, New Jersey, and Florida overlapped significantly both in exposure and onset of illness, while the Washington, D.C., cases emerged some weeks later. This supports the understanding that the attacks took place in two tranches, with letters postmarked 18 September and 9 October.

Seek additional information on the Florida case. Were there any eyewitnesses? Does Blanco remember the envelope? How did the letters travel from New Jersey to their final destinations? Do those modes of transport reveal any clues about additional letters?

Is there any significance to the timing of the letters, either the postmark or the day of the week? Both 18



September and 9 October are Tuesdays. The letter could have been dropped into the mailbox anytime between the last pickup on Monday and Tuesday. Where is the postbox located? What are the surrounding businesses or homes? Are there any cameras in the area?

What about the two outlier cases: Kathy Nguyen in New York and Ottilie Lungren in Connecticut? What explanations are there for these cases? Did any mail destined for these two victims travel via the Hamilton Township mail center in Trenton, New Jersey? There are potentially knowable answers to these questions. Given the uncertainties surrounding the case, it is essential to track down information that would help answer these questions. Investigators never found the source of exposure in the Nguyen case, and they later announced that the Lundgren case was most likely a result of secondary contamination of her mail.

TECHNIQUE 4: PREMORTEM ANALYSIS AND STRUCTURED SELF-CRITIQUE

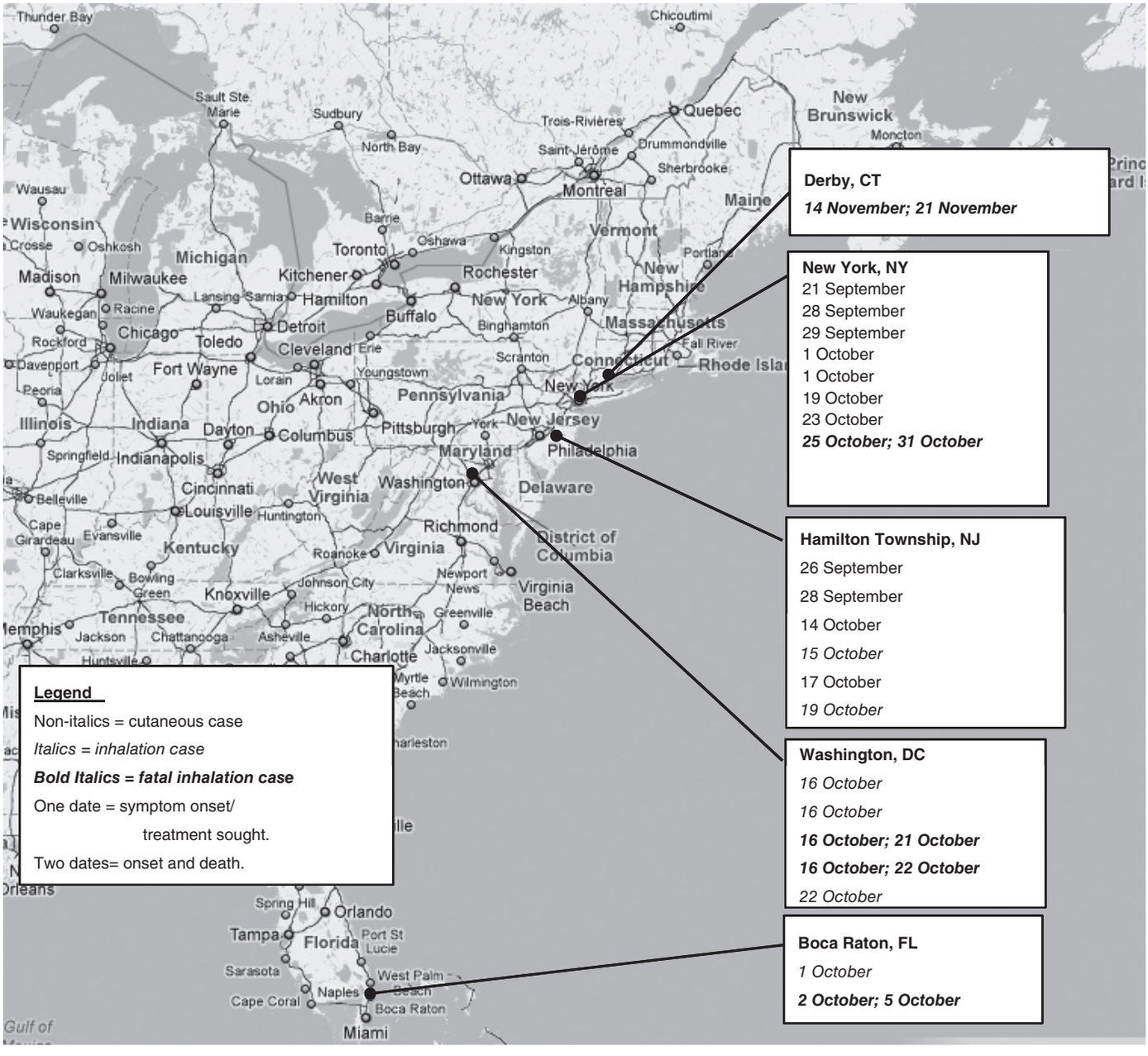
The goal of these techniques is to challenge—actively and explicitly—an established mental model or analytic consensus in order to broaden the range of possible explanations or estimates that are seriously considered. This process helps reduce the risk of analytic failure by identifying and analyzing the features of a potential failure before it occurs.[2]

Task 1.

Conduct a Premortem Analysis Assessment and Structured Self-Critique of the reigning view that Steven Hatfill is the anthrax killer.

Step 1: Imagine that a period of time has passed since you published your analysis that contains the reigning view. You

Map 2.1 ▸ Example of a Map Graphic Depicting the Spatial and Temporal Aspects of the Attacks



suddenly learn from an unimpeachable source that the judgment above was wrong. Then imagine what could have caused the analysis to be wrong.

- One possibility is a problem with the physical evidence in the case. The main physical evidence is the anthrax itself, so any problem with the chain of custody or analysis of the spores could cause a spectacular failure.
- Also, a lack of evidence directly linking Hatfill to the crime could undermine the case.

Step 2: Use a brainstorming technique to identify alternative hypotheses for how the poisoning could have occurred. Keep track of these hypotheses.

- The FBI has taken a painstaking approach to develop a full profile of the killer that stipulates the

Table 2.2 ▶ Common Analytic Pitfalls

Pitfall	Definition
Analytic mindset	A fixed view or attitude that ignores new data inconsistent with that view or attitude
Anchoring	The tendency to rely too heavily on one trait or piece of information when making decisions
Confirmation bias	The tendency to favor information that confirms one's preconceptions or hypotheses, independently of whether they are true
Historical analogy	Using past events as a model to explain current events or to predict future trends
Mirror imaging	Assuming that the subject of the analysis would act in the same way as the analyst
Premature closure	Coming to a conclusion too quickly based on initial and incomplete information
Satisficing	Generating a quick response that satisfies all stakeholders associated with the issue

key criteria required for the killer to produce the anthrax, such as access and scientific expertise. As a result, they have been able to narrow the list of potential persons of interest to less than fifty, and by working to rule out potential suspects. As a result, other possible hypotheses could be that another scientist at the US Army Medical Research Institute of Infectious Diseases (USAMRIID) could be the killer. Also, someone outside the lab could have gained access to the Ames strain through the normal course of scientific inquiry and collaboration. Do any other facilities in the United States have Ames strain anthrax? Does USAMRIID conduct scientific exchanges with foreign countries? These hypotheses point to gaps such as chain of control and security procedures that investigators should fill in order to rule out these other possible explanations.

Step 3: Identify key assumptions underlying the consensus view. Could any of these be unsubstantiated? Do some assumptions need caveats? If some are not valid, how much could this affect the analysis?

Step 4: Review the critical evidence that provides the foundation for the argument. Is the analysis based on any critical item of information? On a particular stream of reporting? If any of this evidence or the source of the reporting turned out to be incorrect, how would this affect the analysis?

- The critical pieces of evidence against Hatfill include:
  - Biology student/currently a virologist
  - Spent time in Africa during anthrax outbreaks
  - Worked at USAMRIID from 1997 to 1999
  - Had "virtually unrestricted access" to USAMRIID facilities
  - Possessed specialized knowledge about how to weaponize bubonic plague
  - Knew how to disseminate anthrax via mail
  - Oversaw construction of a model Iraq mobile bioweapons lab
  - Helped prepare a brochure in 1999 on how to handle anthrax attacks
  - Went to medical school in Zimbabwe near a suburb called Glendale, the same name that was on two of the envelopes
  - Was taking Cipro in September
- Taken together, these form a circumstantial case that raises suspicion about Hatfill.

Step 5: Is there any contradictory or anomalous information? Was any information overlooked that is inconsistent with the lead hypothesis?

- Hatfill is a virologist—an expert in viruses such as Ebola, HIV, hemorrhagic fever, etc.—not a microbiologist who has expertise in bacteria. There is no evidence that he has the requisite skills to produce highly purified anthrax spores of this strain.
- The FBI profile describes the suspect as an introverted "person who prefers being by himself more often than not," but Hatfill is an extroverted ex–military member who has lived and worked overseas in Africa for most of his life.

Step 6: Is there a potential for deception? Does anyone have motive, opportunity, and means to deceive you?

- Any of the scientists under scrutiny have motive, opportunity, and means to deceive investigators who are not scientific experts themselves. If a scientist other than Hatfill at USAMRIID or elsewhere were the true killer, that person would certainly seek to minimize his or her own profile, perhaps even by assisting investigators or falsely identifying Hatfill as the main suspect.

Step 7: Is there an absence of evidence, and does it influence the key judgment?

- There is no physical evidence that we know of linking Hatfill to the anthrax. There is physical evidence

linking the anthrax to USAMRIID. This lack of evidence should challenge the level of certainty that Hatfill should be named as a person of interest until the circumstantial evidence can be thoroughly reviewed.

- Neither is there evidence, either direct or indirect, linking Hatfill to NBC or Tom Brokaw, the *New York Post,* or Senators Daschle and Leahy.

Step 8: Have you considered the presence of common analytic pitfalls such as analytic mindsets, confirmation bias, "satisficing," premature closure, anchoring, and historical analogy?

- *Confirmation bias.* The case against Hatfill could represent confirmation bias. No physical evidence links Hatfill to the crime, yet he is publicly named a person of interest. The evidence against him is entirely circumstantial and deserves greater scrutiny. The presence of several pieces of circumstantial evidence that the government found once it focused on him as a suspect may have had the unintended consequence of raising the government's confidence in Hatfill's guilt. As a result, each piece of evidence deserves greater scrutiny to ensure that the decision to name Hatfill as a person of interest is not a result of confirmation bias. For example, are there alternative explanations for why Hatfill was taking Cipro in 2001?

- *Satisficing/Premature Closure.* The government interviewed Hatfill and searched his home on 25 June. No charges were brought against him at that time. As pressure mounted to identify the perpetrator, however, the government again searched his home on 1 August. Pressure—whether explicit or implicit—may have caused investigators to come to the first, most plausible explanation (satisficing) without fully investigating the other possible suspects or tracking down questions about circumstantial or anomalous evidence (premature closure). In law enforcement spheres, this is called detective myopia.

Step 9: Based on the answers to the themes of inquiry just outlined, list the potential deficiencies in the argument in order of potential impact on the analysis.

- The lack of physical evidence linking Hatfill to the crime raises uncertainty about his guilt, even in the face of other circumstantial evidence.
- Each of the points above can be used to develop a prioritized collection strategy to obtain information that would help corroborate or refute the questions raised by the Premortem Analysis and Structured Self-Critique.

Analytic Value Added: As a result of your analysis, what are the strengths and weakness of the case against Hatfill? What additional information should you seek out? Do any assumptions underpin the case? Do they change or reinforce your level of certainty? The case against Steven Hatfill is based on several pieces of circumstantial evidence that, taken together, could indicate he is the anthrax killer. They could also simply form a house of cards that will collapse upon further scrutiny. For example, the evidence that he was taking Cipro in September could indicate that he was using the drug as a prophylactic measure for anthrax exposure, but he could also have been taking it for a common infection. A potentially key deficiency in the case against Hatfill surrounds his access to the Ames strain anthrax stored at USAMRIID. Until this assumption is substantiated, it raises uncertainty about Hatfill's access to the material and any role he could have played in the attacks. Also, it is unclear what Hatfill's motive could have been; and, if he was trained as a virologist, he may have lacked the expertise to produce highly purified and dried anthrax spores.

CONCLUSION

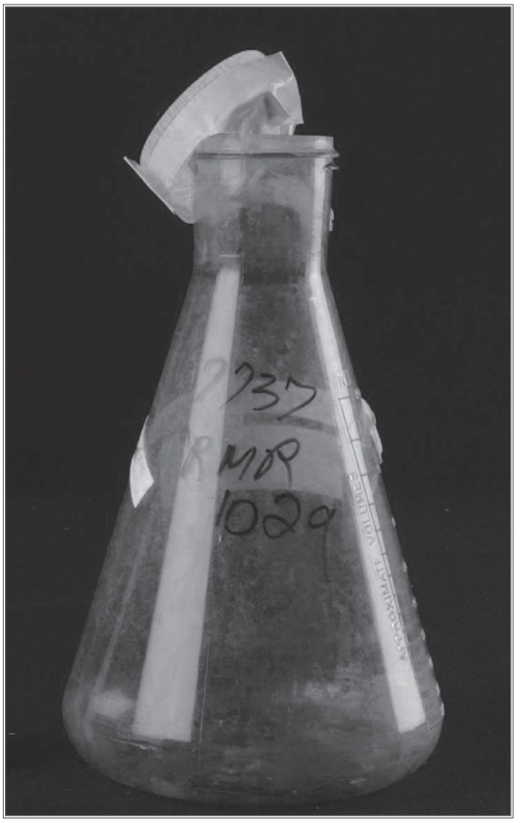
On 8 August 2008, the government officially excluded Steven J. Hatfill as a suspect. The announcement came two weeks after the Department of Justice settled an invasion of privacy lawsuit by Hatfill for over $5 million. This was one of several lawsuits brought by Hatfill against the government and media in connection with the media frenzy surrounding his identification as a person of interest.[3] The courts dismissed several libel suits brought by Hatfill, including one against the *New York Times.* According to a letter the Department of Justice sent to Hatfill's lawyer, the government "concluded, based on lab access records, witness accounts, and other information, that Dr. Hatfill did not have access to the particular anthrax used in the attacks, and that he was not involved in the anthrax mailings."[4] Some of the most anomalous evidence was easily explained:

Hatfill had chronic sinus infections for years as a result of an injury sustained while serving as a volunteer medic in Africa, and he took Cipro to manage the infection. He never had access to the BLS-3 lab at USAMRIID, a fact supported by the lab access records. Also, he completed his doctoral research but left Africa before receiving his diploma.[5] In the end, new scientific methods developed after the attacks and in conjunction with the case helped to prove Hatfill's innocence. In 2007, investigators had used new genetic methods to determine that a flask of "RMR-1029" Ames strain anthrax found at USAMRIID was the parent material for the anthrax spores. According to the Department of Justice Amerithrax Investigative Summary, investigators subsequently were able to rule out Hatfill as a suspect because:

> Early in the investigation, it was assumed that isolates of the Ames strain were accessible to any individual at USAMRIID with access to the bio-containment lab. Later in the investigation, when scientific breakthroughs led investigators to conclude that RMR-1029 was the parent material to the anthrax powder used in the mailings, it was determined that Dr. Hatfill could not have been the mailer because he never had access to the particular bio-containment suites at USAMRIID that held the RMR-1029. In other words, although Dr. Hatfill had access to Ames strain anthrax while at USAMRIID, he never had access to the particular spore-batch used in the mailings.[6]

Other scientists at USAMRIID did have access to the RMR-1029 Ames strain anthrax, but only a very limited number. Investigators used traditional law enforcement methods such as interviews, alibi checks, and polygraphs to rule out all but one suspect: the very scientist who had developed RMR-1029 and who had been aiding the investigation from the start, Dr. Bruce Ivins. As investigators prepared to seek authorization to ask a federal grand jury to return an indictment charging Dr. Ivins with Use of a Weapon of Mass Destruction in violation of Title 18, United States Code 2332a and related charges, Ivins took a lethal dose of Tylenol and died on 29 July 2008.[7]

Investigators indicated that Ivins had motive, opportunity, and means to commit the crime, in addition to suffering from severe mental health issues. They found that Ivins was "under intense personal and professional pressure" because the anthrax vaccine program to which he had devoted his career was failing. "Short of some major breakthrough or intervention, he feared that the vaccine research program was going to be discontinued. Following the anthrax attacks, his program was suddenly rejuvenated."[8]



Flask of RMR-1029 found in Ivins's Lab
SOURCE: Courtesy of the Department of Justice.

Not only had Ivins developed the spore batch for RMR-1029, laboratory logs indicated that he had spent an abnormal number of late-night and off-hours in his lab, where the RMR-1029 was stored along with highly sophisticated lab equipment capable of creating the anthrax powder. He was one of "the few researchers nationwide with the knowledge and ability to create the highly purified spores used in the mailings."[9]

In addition, the envelopes used in the mailings were prestamped envelopes from a batch distributed only to post offices in Maryland and Virginia. Investigators found that the "envelopes most similar to those used in the attacks" were distributed to the Frederick, Maryland, post office that was only blocks from Ivins's home. He also took steps to cover his tracks: he decontaminated his office and failed to report it; sent nonsensical explanations for the first inhalation anthrax case to the Centers for Disease Control,

presumably to throw investigators off his trail; threw out a book on codes that he may have used to embed codes into the anthrax letters; and gave the FBI "questionable" samples of RMR-1029 in order to conceal his activities from investigators.[10]

Investigators also pointed to Ivins's mental health status, noting his use of alternate identities, his 40-year-long obsession with the Kappa Kappa Gamma (KKG) sorority during which he burglarized chapter houses, and his inability to explain his own suspicious behavior. The task force found that not only were the anthrax letters sent from a New Jersey mailbox outside a KKG chapter at Princeton University, but also Ivins "was unable to provide reasonable or consistent explanations for his behavior, such as his late night hours and submission of questionable samples of RMR-1029."[11]

Still, given Ivins's untimely death, and the fact that the government could not take the case to trial, not everyone accepted the government's explanations. Ivins's lawyers posthumously defended their client, calling the charges "heaps of innuendo" and "a total absence of proof that he committed this crime."[12] Some of his colleagues accused the government of "hounding an innocent man to suicide."[13] Later, when the government closed the case in February 2010 and released to the public thousands of documents related to the case, his colleagues still raised doubts that he could have perpetrated the crime. In an email quoted in the documents released by the government, Ivins posthumously offers his own explanation for some of his erratic behavior, blaming an alter ego, "Crazy Bruce, who surfaces periodically as paranoid, severely depressed and ridden with incredible anxiety."[14]

Over a decade after the attacks, questions still remain. A 2010 report by the National Research Council found that it "is not possible to reach a definitive conclusion about the origins of the anthrax in letters mailed to New York City and Washington, D.C., based solely on the available scientific evidence."[15] The report specifically calls into question the RMR-1029 flask, indicating that while the anthrax in the letters and the flask "share a number of genetic similarities . . . the committee found that other possible explanations for the similarities—such as independent, parallel evolution—were not definitively explored during the investigation."[16] Also, while the RMR-1029 flask was identified as the "parent material" for the anthrax in the letters, the National Academy of Sciences' report indicated that it "was not the immediate source of spores used in the letters," noting, "the contents of the New York and Washington letters had different physical properties."[17]

The FBI, however, is confident that it found its anthrax killer. In response to questions about the science behind the case that were raised by the National Research Council report, the FBI reiterated the point from the report "that it was not possible to reach a definitive conclusion about the origins of the samples based on science alone," and added that, even so, "investigators and prosecutors have long maintained that while science played a significant role, it was the totality of the investigative process that ultimately determined the outcome of the anthrax case."[18] Despite ongoing questions surrounding Ivins's guilt and the science behind the investigation, the case remains closed.

KEY TAKEAWAYS

- Chronologies and Timelines are useful tools for tracking key events and evidence. They help individual analysts organize their thinking and provide a transparent framework for groups of analysts to track the progress of a case. They are particularly useful for identifying gaps and putting fast-breaking events in context.
- Use the Premortem Analysis and Structured Self-Critique to troubleshoot your analysis and avoid a rush to judgment. The technique will help you identify assumptions, biases, and evidentiary inconsistencies that otherwise could undermine the analysis.

NOTES

1. "Amerithrax Investigative Summary," Department of Justice, February 19, 2010, www.justice.gov/amerithrax, 3.

2. The steps as outlined in this case combine the processes for a Premortem Analysis and Structured Self-Critique. This combination is particularly helpful in cases that require analysts to think broadly, imaginatively, and exhaustively about how they might have been wrong. The Premortem Analysis taps the creative brainstorming process, and the Structured Self-Critique

provides a step-by-step assessment of each analytic element. To aid students' learning process, the questions in this case have already been narrowed from the fuller set of Structured Self-Critique questions found in Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, DC: CQ Press, 2011).

3. Hoyt Clark, "Headlines and Exonerations," *New York Times,* August 17, 2008, http://www.lexisnexis.com.ezproxy.umuc.edu/hottopics/lnacademic.

4. Carrie Johnson Warrick, "Prosecutors Clear Hatfill in Anthrax Case," *Washington Post,* August 9, 2008, http://www.lexisnexis.com.ezproxy.umuc.edu/hottopics/lnacademic.

5. Steven J. Hatfill, discussion with the author, February 24, 2012.

6. "Amerithrax Investigation Summary," 6.

7. Ibid., 1.

8. Ibid., 8.

9. Ibid.

10. Ibid., 9.

11. Ibid., 10.

12. Scott Shane and Eric Lichtenblau, "F.B.I. Presents Anthrax Case, Saying Scientist Acted Alone," *New York Times,* August 7, 2008, http://www.nytimes.com/2008/08/07/washington/07anthrax.html?ref=science& page wanted=print.

13. Ibid.

14. Scott Shane, "F.B.I., Laying Out Evidence, Closes Anthrax Case," *New York Times*, February 19, 2010, http://www.nytimes.com/2010/02/20/us/20anthrax.html?ref=science&pagewanted=print.

15. "Science Alone Does Not Establish Source of Anthrax Used in 2001 Mailings," *National Academy of Sciences*, February 15, 2011, http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=13098.

16. Ibid.

17. Ibid.

18. Michael P. Kortan "The Anthrax Investigation: The View from the F.B.I," *New York Times*, October 27, 2011, http://www.nytimes.com/2011/10/28/opinion/the-anthrax-investigation-the-view-from-the-fbi.html?_r=1&ref=anthrax&pagewanted=print.

Table 3.1 ▶ Case Snapshot: Cyber H_20		
Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Getting Started Checklist	p. 47	Decomposition and Visualization
Key Assumptions Check	p. 209	Assessment of Cause and Effect
Devil's Advocacy	p. 260	Challenge Analysis

3 Cyber H_20
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

Analysts are often asked to conduct their analyses under tight time frames on breaking issues. In situations where time is of the essence and the pressure to deliver the analysis to stakeholders is high, the onus is on analysts to ensure that relevance and accuracy are not sacrificed for timeliness. The Getting Started Checklist, Key Assumptions Check, and Devil's Advocacy are quick and effective techniques that help analysts to focus on the relevant questions, consider alternative outcomes, reveal unsupported assumptions, and troubleshoot their final analysis.

In this case, analysts must contend not only with the pressure to produce an analytic product quickly, but also with the insufficiency of the evidence at hand, the presence of unchallenged assumptions in the initial analytic judgment, and the need for information sharing and collection with other stakeholders. Each of the techniques utilizes a different approach to troubleshoot these aspects of the analysis. Once analysts have uncovered one or two deficiencies with the initial judgment, they may be tempted to address only these and move on. The presence of three techniques that emphasize different aspects of the analysis encourages analysts to overcome this temptation by thoroughly examining the problem through various prisms afforded by the techniques. The result is a much more nuanced and thorough understanding of the problem, impact, stakeholders, underlying assumptions, information gaps, and evidentiary base.

TECHNIQUE 1: GETTING STARTED CHECKLIST

Getting off to the right start is key to any successful analysis. The Getting Started Checklist can help to explicate important aspects regarding the audience, central analytic question, evidentiary base, alternative explanations, and other resources that could be brought to bear on the problem. By getting these fundamentals correct at the start of a project, analysts can avoid having to change course later on. This groundwork can save time and greatly improve the quality of the final product.

Task 1.

Put yourself in the shoes of the Illinois Statewide Terrorism and Intelligence Center analysts who have just learned about the pump incident at the Curran-Gardner water plant. Use the following Getting Started Checklist questions to launch your analysis:

Step 1: What has prompted the need for the analysis? For example, was it a news report, a new intelligence report, a new development, a perception of change, or a customer request?

This analysis was prompted by a new development on the basis of a report by Curran-Gardner to the EPA. The fusion center is responsible for analysis and information sharing with federal, state, local, tribal, and industry stakeholders.

Step 2: What is the key question that needs to be answered? What caused the pump to fail?

Step 3: Why is this issue important, and how can analysis make a meaningful contribution?

This issue is important because one possible explanation is that the supervisory control and data acquisition (SCADA) system has been remotely accessed and controlled

via a foreign-based IP address. The implications of this are far-reaching because it would be the first such reported incident and could signal a new trend in activity that could have reverberations across not only the water sector, but also other sectors that utilize industrial control systems.

Step 4: Has your organization or any other organization ever answered this question or a similar question before, and, if so, what was said? To whom was this analysis delivered, and what has changed since that time?

This is a first for the water sector and for US infrastructure, but there have been other instances, such as in Australia, in which an insider has compromised a waste water system.

Step 5: Who are the principal customers? Are these customers' needs well understood? If not, try to gain a better understanding of their needs and the style of the reporting they like.

The customer set includes federal, state, and local officials, as well as industry. At the federal level, interest will be high because of the possible implications of such an attack for other types of infrastructure, the broader economic impact, and the potential national security implications. At the state and local level, interests will center on the implications for the water customers and the economic effects. Industry will be interested in all of these issues.

Step 6: Are there other stakeholders who would have an interest in the answer to this question? Who might see the issue from a different perspective and prefer that a different question be answered? Consider meeting with others who see the question from a different perspective.

At the federal level, DHS Cyber Emergency Response Team (CERT) is an important resource for cyberforensics. At the industry level, the WaterISAC may have expertise that could be brought to bear. The Curran-Gardner employees and contract staff may also be able to provide more context for analysts regarding the timing, location, pump type, and SCADA system logs.

Step 7: From your first impressions, what are all the possible answers to this question? For example, what alternative explanations or outcomes should be considered before making an analytic judgment on the issue?

While the initial reports suggest that a hacker caused the pump failure, other possible explanations could include a cyber-savvy insider or a mechanical failure.

Step 8: Depending on responses to the previous questions, consider rewording the key question. Consider adding subordinate or supplemental questions.

What is the most likely cause of the pump failure?

What does the range of possible causes mean for Curran-Gardner's customers?

What does it mean for industrial control system security more broadly?

Step 9: Generate a list of potential sources or streams of reporting to be explored.

- Curran-Gardner staff and contractors
- WaterISAC
- DHS CERT
- Previous reporting on tests, experiments, known intrusions for other sectors

Step 10: Reach out and tap into the experience and expertise of analysts in other organizations—both within and outside government—who are knowledgeable on this topic. For example, call a meeting or conduct a virtual meeting to brainstorm relevant evidence and to develop a list of alternative hypotheses, driving forces, key indicators, or important players.

Consider convening a teleconference with DHS CERT, the WaterISAC, and knowledgeable Intelligence Community professionals who may be able to help provide context about the threat environment, suggest new sources of information, or brainstorm possible hypotheses or driving forces.

Analytic Value Added: **How do the answers to the questions listed affect the prevailing judgment that the pump failure was caused by a Russian-based intrusion using stolen SCADA system log-on credentials?** The Getting Started Checklist suggests that more work is needed before publication, such as reaching out to knowledgeable stakeholders in industry and government who may have relevant knowledge or expertise, seeking additional information about the incident from Curran-Gardner employees and contract staff, and more closely examining other possible explanations for the pump failure.

TECHNIQUE 2: KEY ASSUMPTIONS CHECK

The Key Assumptions Check is a systematic effort to make explicit and question the assumptions that guide an analyst's

interpretation of evidence and reasoning about any particular problem. Assumptions are usually a necessary and unavoidable means of filling gaps in the incomplete, ambiguous, and sometimes deceptive information with which the analyst must work. They are driven by the analyst's education, training, and experience, including the cultural and organizational contexts in which the analyst lives and works. It can be difficult to identify assumptions, because many are sociocultural beliefs that are unconsciously or so firmly held that they are assumed to be truth and not subject to challenge. Nonetheless, identifying key assumptions and assessing the overall impact should they be invalid are critical parts of a robust analytic process.

Task 2.

Conduct a Key Assumptions Check of the prevailing judgment that the pump failure was caused by a Russian-based intrusion using stolen SCADA system log-on credentials.

Step 1: Gather a small group of individuals who are working on the issue along with a few "outsiders." The primary analytic unit already is working from an established mental model, so the "outsiders" are needed to bring other perspectives.

Step 2: Ideally, participants should be asked to bring a list of assumptions when they come to the meeting. If not, start the meeting with a silent brainstorming session. Ask each participant to write down several assumptions on 3 x 5 cards.

Step 3: Collect the cards and list the assumptions on a whiteboard for all to see. A simple template can be used, as shown in Table 3.2.

Step 4: Elicit additional assumptions. Work from the prevailing analytic line back to the key arguments that support it. Use various devices to help prod participants' thinking. Ask the standard journalistic questions: Who? What? How? When? Where? and Why?

Phrases such as "will always," "will never," or "would have to be" suggest that an idea is not being challenged and perhaps should be. Phrases such as "based on" or "generally the case" usually suggest that a challengeable assumption is being made.

Step 5: After identifying a full set of assumptions, critically examine each assumption. Ask:

- Why am I confident that this assumption is correct?
- In what circumstances might this assumption be untrue?
- Could it have been true in the past but no longer be true today?
- How much confidence do I have that this assumption is valid?
- If the assumption turns out to be invalid, how much impact would this have on the analysis?

Step 6: Using Table 3.2, place each assumption in one of three categories:

1. Basically supported
2. Correct with some caveats
3. Unsupported or questionable—the "key uncertainties"

Step 7: Refine the list, deleting those assumptions that do not hold up to scrutiny and adding new assumptions that emerge from the discussion.

Table 3.2 ▶ Key Assumptions Check Template

Key Assumption	Commentary	Solid	With Caveat	Unsupported

Table 3.3 ▶ Cyber H_20 Key Assumptions Check Example

Key Assumption	Commentary	Supported	With Caveat	Unsupported
The pump failure was a result of a computer network attack originating in Russia.	There are other possible explanations for the failure that do not include a computer network attack originating in Russia, such as an insider or a mechanical failure. There is no direct reporting that indicates the failure was a result of an attack.			X
The Russian IP address and user log-on in the SCADA log indicate that the hacker used stolen log-on credentials.	The Russian IP address simply indicates that it was the last IP address used to access the system. Hackers based somewhere else could have bounced off the IP address in order to obfuscate their true location. This person could be not only a Russian-based hacker, but also a computer-savvy insider who used his or her own log-on credentials, or someone based in a third country who stole the credentials.			X
The information reported to the EPA is a sufficient basis to rule out other possible causes.	The information reported to the EPA is a starting point, but we cannot assume that this information is accurate or exhaustive at this point.			X

Steps 8: Consider whether key uncertainties should be converted into collection requirements or research topics.

Analytic Value Added: What impact could unsupported assumptions have on your analysis of the pump failure? How confident are you in your analysis of the cause of the failure? All of the unsupported assumptions could have an impact on the original analysis of the pump failure (see Table 3.3). Most important, the assumption that the SCADA system log-on information indicates a Russian-based intrusion using stolen credentials is particularly perilous because there are a number of other possible explanations for the activity. All of the unsupported assumptions should, therefore, be treated as collection requirements prior to publication; or, at the very least, the analysis should be amended to reflect these uncertainties.

TECHNIQUE 3: DEVIL'S ADVOCACY

Devil's Advocacy can be used to critique a proposed analytic judgment, plan, or decision. Devil's Advocacy is often used before a final decision is made, when a policy maker or military commander asks for an analysis of what could go wrong. The Devil's Advocate builds the strongest possible case against the proposed decision or analytic judgment, often by examining critical assumptions and sources of uncertainty, among other issues.

Task 3.

Build the strongest possible case against the prevailing judgment that the pump failure was caused by a Russian-based intrusion using stolen SCADA system log-on credentials.

Steps: Although there is no prescribed procedure for a Devil's Advocacy, begin with the analytic judgment, assumptions, and gaps. These can serve as a useful starting point from which to build the case against the original judgment that the pump failure was caused by a Russian-based intrusion using stolen SCADA system log-on credentials. Next, build a logical argument that undermines each goal.

It is too early to conclude that the pump failure was caused by a Russian-based intrusion using stolen SCADA system log-on credentials. The basis for the judgment is an unsupported assumption that the so-called attack originated in Russia and was conducted using stolen log-on credentials. While previous government- and industry-sponsored experiments have demonstrated this capability on the part of hackers, we cannot rule out other possible explanations at this time. Barring further investigation and collection of information from the site of the pump failure and US government cyberforensic specialists, it is just as likely that the cause of the failure is attributable to an insider or a simple equipment malfunction.

Analytic Value Added: Which issues could undermine the analysis, and why? Unsupported assumptions and

critical information gaps raise the level of uncertainty about the initial analysis. Given that a case can be made that undermines this initial analysis even in the absence of additional information, analysts should reserve judgment or caveat their analysis to reflect the deep level of uncertainty about the cause of the pump failure. Using the results of the Devil's Advocacy, analysts can create a collection requirements list that would help them to rule out other causes. Doing so could help raise or lower the level of uncertainty about the actual cause of the pump failure.

CONCLUSION

On 10 November 2012, just two days after the pump failure at the Curran-Gardner plant, the Illinois Statewide Terrorism and Intelligence Center issued a Daily Intelligence Notes report entitled "Public Water District Cyber Intrusion." The report "detailed initial findings of anomalous behavior in a supervisory control and data acquisition (SCADA) system at a Central Illinois public water district." This report also alleged a malicious cyber intrusion from an IP address located in Russia that caused the SCADA system to power on and off, resulting in a water pump to burn out.[1] Joe Weiss, a well-known computer engineer, broke the story when he posted information about the report on his blog and spoke to press outlets, warning, "there very easily could be other utilities as we speak who have their networks compromised."[2] The media reported the failure as the first-ever US SCADA system attack, akin to the Stuxnet attack that targeted the industrial control system at Iran's Bushehr nuclear power plant. Within two weeks, and after intense scrutiny by the media, the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and water sector stakeholders, however, DHS reported that the pump had failed "because of physical and mechanical issues over a period of time rather than from a cyber attack."[3]

During the two-day period between the initial pump failure and the publication of the fusion center report, the failure to challenge faulty assumptions and missed opportunities to share and corroborate information seem to have produced a perfect storm. When the pump failed, a Curran-Gardner employee requested help from a computer repairman, who subsequently reviewed the SCADA system logs and noted that the system had been remotely accessed by a system username via a Russian IP address during the preceding months. Curran-Gardner reported the information to the Environmental Protection Agency, which is the lead sector-specific agency, and the information made its way to the Illinois Statewide Terrorism and Intelligence Center. The fusion center, just two days later, released the report, indicating that the event was caused by a Russian-based intrusion using stolen SCADA system log-on credentials.[4] It is unclear whether the Curran-Gardner employee, the computer repairman, or the fusion center made the judgment that the failure was linked to the remote access from Russia, and that this represented an intrusion using stolen credentials.

The DHS computer forensic specialists at the CERT learned about the incident a week later, on 16 November.[5] Upon subsequent on-site analysis of the logs, CERT "could not validate the claims made in the report," according to a joint DHS–FBI statement that was issued on 22 November.[6] The user whose username appeared in the log alongside the Russian IP address and who was an employee of the SCADA system maintenance company used by Curran-Gardner was not consulted. The user, Jim Mimlitz, later told a popular technology magazine, "I could have straightened it up with just one phone call."[7] Mimlitz was on vacation in Russia in June 2011 when he received a cell phone call asking him to examine the SCADA computer at Curran-Gardner. He did so using remote access from Russia, and again on a flight layover in Germany. The so-called account breach was actually the user himself. After reading about the intrusion in the press, Mimlitz realized what had happened. He worked with the CERT team to scour the logs and found that all indications pointed to an electromechanical problem as the source of the pump failure, not a SCADA system problem. In addition, Mimlitz told the press that the system instability, or "glitches" noted by the plant in the months preceding the problem, were actually due to the age of the system and modifications that had been made a year earlier by another contractor.[8]

On 22 November, the industry-run WaterISAC released a bulletin stating, "after detailed analysis, DHS and FBI have found no evidence of a cyber intrusion into the SCADA system of the Curran-Gardner Public Water District in Springfield."[9] In an ICS–CERT Information Bulletin released on 23 November, the DHS and FBI confirmed:

> In addition, there is no evidence to support claims made in the initial Illinois STIC report—which was based on raw, unconfirmed data and subsequently leaked to the media—that any credentials were stolen, or that the vendor was involved in any malicious activity that led to a pump failure at the water plant. In addition, DHS and

the FBI have concluded that there was no malicious or unauthorized traffic from Russia or any foreign entities, as previously reported.[10]

Luckily for Curran-Gardner's 2,000 customers, the ICS–CERT bulletin also noted, "At no time were there any impacts to customers served by the water district due to the pump failure."[11]

KEY TAKEAWAYS

- Before you write, use the Getting Started Checklist to ensure that you have fully considered the question, alternative explanations, assumptions, gaps, evidentiary base, and stakeholders to be consulted. Doing so can save time and lead to a more productive and thorough analysis.
- A Key Assumptions Check is a vital part of any analysis. Use it not only to identify unsupported assumptions, but also to explore how changes in your assumptions could affect your bottom-line judgments. A Key Assumptions Check will also help you identify what information is needed to raise or lower your confidence in in your analysis.
- When the stakes are high, but time is short, use Devil's Advocacy as a quick and effective way to find holes in your logic or judgments that are not well supported by the facts.

NOTES

1. "ICSB-11-327-01—Illinois Water Pump Failure Report," Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team, November 23, 2011, http://www.us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf.
2. Ibid.
3. "ICS-CERT Monthly Monitor, Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team," December 2011, http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Dec2011.pdf.
4. Kim Zetter, "Exclusive: Comedy of Errors Led to False 'Water-Pump Hack' Report," *Wired*, November 30, 2011, http://www.wired.com/threatlevel/2011/11/water-pump-hack-mystery-solved.
5. "ICS–CERT and FBI Statements on Water System Attacks," InfosecIsland, November 22, 2011, http://www.infosecisland.com/blogview/18303-ICS-CERT-and-FBI-Statements-on-Water-System-Attacks.html.
6. Ibid.
7. Zetter, "Exclusive: Comedy of Errors Led to False 'Water-Pump Hack' Report."
8. Ibid.
9. Mickey McCarter, "Infrastructure Security: DHS, FBI Dispel Allegations of Illinois Water Pump Attack," *Homeland Security Today*, November 30, 2012, http://www.hstoday.us/focused-topics/infrastructure-security/single-article-page/dhs-fbi-dispel-allegations-of-illinois-water-pump-hack.html.
10. ICSB-11-327-01—Illinois Water Pump Failure Report," Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team, November 23, 2011, http://www.us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf.
11. Ibid.

Table 4.1 ▶ Case Snapshot: Is Wen Ho Lee a Spy?		
Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Force Field Analysis	p. 304	Decision Support
Deception Detection	p. 198	Hypothesis Generation and Testing
Premortem Analysis	p. 240	Challenge Analysis
Structured Self-Critique	p. 245	Challenge Analysis

4 Is Wen Ho Lee a Spy?
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

Using this case, analysts can build a good argument that Wen Ho Lee is a spy. They can also build a good argument that he is not a spy. This case illustrates how important it is for analysts to consider all the data, not simply build a case to suit their perspective. The techniques in this case help analysts evaluate both sides of the argument about Wen Ho Lee's activities, dig deeper into the possibility of deception surrounding a key piece of evidence—the walk-in document—that catalyzed the case again him, and troubleshoot their final analysis by conducting a Premortem Analysis. This combination of techniques helps analysts identify important assumptions, gaps, and avenues for further research that can improve the overall rigor of their analysis and avoid the temptation to "go with their gut," especially when doing so can have such significant consequences.

TECHNIQUE 1: FORCE FIELD ANALYSIS

A Force Field Analysis helps analysts identify and assess all of the forces and factors for and against an outcome and avoid premature or unwarranted focus only on one side of the analysis. It is particularly helpful at the beginning of a project or investigation as a tool to sort and consider all evidence as an evidentiary base is amassed. Furthermore, the weighting mechanism allows analysts to more easily identify the strongest and weakest forces or factors and recommend strategies to reduce or strengthen the effect of forces that support or work toward a given outcome.

In this case, investigators amassed a long list of counts against Wen Ho Lee, but Lee pled guilty to—and was convicted of—only one relatively minor count of mishandling a controlled document. Many observers questioned the government's case; the government remained solid in its conviction that Wen Ho Lee was a spy. A Force Field Analysis helps to illuminate both sides of the case.

Task 1.

Conduct a Force Field Analysis of the arguments for and against Wen Ho Lee being guilty of passing nuclear secrets to China.

Step 1: Define the problem, goal, or change clearly and concisely.

Step 2: Use form of brainstorming to identify the main factors that will influence the issue.

Two key considerations would be Wen Ho Lee's ethnic loyalty to China and a history of interactions—some of them unreported—with Chinese scientists. Note, however, that Lee was of Taiwanese descent, and this could influence how he views his relationship with the mainland. Some would argue that Hu Side's hug of Lee and praise for Lee's help indicated that Lee was providing valuable information to the Chinese. However, if Lee had been a clandestine source, it is unlikely that the Chinese government would have wanted to draw undue attention to its relationship with Lee.

Another key factor is the lack of any hard evidence of espionage; Lee was never observed providing any materials to the Chinese, nor was he overheard revealing any secrets. Lee and his wife served as informants for the FBI. Some would argue this proved his loyalty, while others would say he was operating as a double agent and that serving as an informant provided him with a good feedback channel.

There is no doubt that Lee moved large quantities of data from a classified computer to an unclassified computer. The question is why. Was he told to archive the data? Was he afraid of losing his job and did he want to keep a copy of his "notes"? Did he put the data on tape drives to pass to the Chinese? Although Lee requested remote access to a classified system while in Taiwan, he did not do so surreptitiously. Some would point to his questionable security practices as evidence that he was trying to conceal clandestine activities; others would point out that he was simply absentminded.

The case study does not include information about Lee's financial situation or whether his colleagues at the lab exhibited similar behavior and security lapses. Neither does the case contain any information about Wen Ho Lee's attitude toward the management at Los Alamos National Laboratory (LANL) nor whether he felt denied opportunity or otherwise disadvantaged. These potential driving forces would be topics of investigation and analysis and at the very least represent gaps that should be discussed.

Step 3: Make one list showing the strongest arguments supporting Wen Ho Lee's innocence and another list showing the strongest arguments showing his guilt.

Step 4: Array the lists in a table like Table 4.2 in the book. Table 4.5 shows an example response.

Step 5: Assign a value to each factor or argument for and against to indicate its strength. Assign the weakest-intensity scores a value of 1 and the strongest a value of 5. The same intensity score can be assigned to more than one factor if you consider the factors equal in strength.

Step 6: Calculate a total score for each list to determine whether the arguments for or against are dominant.

In this case, the total points arguing for his guilt are 17 and for innocence are 20. It should be noted that this does not necessarily mean that he is innocent. If other factors are added to the "Arguments For" column, the overall score would increase. For this reason, it is important to maintain some balance in terms of how many factors are included on each list. In some cases, even one factor could make the case compelling, for example, if Wen Ho Lee had confessed that he had committed espionage when being interrogated.

Step 7: Examine the two lists to determine whether any of the factors balance each other out.

In addition to the Hu Side hug, the question of Lee's loyalties to China or Taiwan balance out. Our assessment might change if we had additional information that Lee was observed making public anti-China statements or, contrarily, that most of his family still resided on the mainland and he maintained close ties to them.

Table 4.5 ▶ Wen Ho Lee Force Field Analysis Example

Issue: Wen Ho Lee Is a Chinese Spy			
Weight	Arguments For	Arguments Against	Weight
3	China targets ethnic Chinese Americans.	Lee is Taiwanese American.	3
4	Frequent contacts with high-level Chinese nuclear scientists.	Lee and his wife were FBI informants.	4
2	Did not report contacts with Chinese; failed to get clearance to pass an unclassified document to the Taiwanese.	No evidence that Lee passed any documents or tapes to China.	5
2	Tried to get remote access via the help desk to a classified computer network while in Taiwan.	Chinese able to obtain most information from unclassified sources.	3
3	When visiting LANL, Hu Side hugged Lee and thanked him for his help.	When visiting LANL, Hu Side hugged Lee and thanked him for his help.	3
3	Lee took the PARD data on the tapes home.	Lee was asked to archive the data.	2
?	Financial trouble?		
Total			Total
17			20

Step 8: Analyze the lists to determine how changes in factors might affect the overall outcome. If the technique is being used as a decision tool, devise a manageable course of action to strengthen those forces that lead to the preferred outcome and weaken the forces that would hinder the desired outcome.

Analytic Value Added: **What are the strongest arguments for and against Lee's guilt in your analysis of the issue? Do any factors deserve further investigation? Have you identified any information gaps that should be further investigated?** Strong arguments can be made both for and against Wen Ho Lee's guilt. The US government was unable to substantiate a case that he committed espionage, but some of his behavior (like going home to erase computer documents) suggested that he was feeling guilty about or afraid of something. Viable alternative explanations for Wen Ho Lee's behavior include that he was:

- Simply a sloppy scientist, just like his peers at the lab who often overlook security regulations because they are too focused on their research.
- Part of a "soft spy" network that provided unclassified information to the Chinese but never engaged in espionage.
- Afraid of losing his job and wanted to retain access to files that documented his research activities should they prove useful in a new job.
- Dutifully archiving records as instructed, needing to move the files from a classified to an unclassified system because the classified system did not have any tape drives.

In this case, several key information gaps can be identified that would help investigators resolve the case, including Lee's financial situation and any evidence of unexplained wealth, whether his security lapses were serious breaches or similar to the behavior of most of his colleagues, exactly what materials were downloaded from the classified system, and the extent of his ties to mainland China.

TECHNIQUE 2: DECEPTION DETECTION

Analysts should routinely consider the possibility that adversaries are attempting to mislead them or to hide important information. The possibility of deception cannot be rejected simply because there is no evidence of it; if deception is well done, one should not expect to see evidence of it. There are, however, some indicators that should alert analysts that they may be the targets of deception, such as the timing of reporting or the bona fides of a source, or when there are known and potentially serious consequences if the source is believed.

For illustrative purposes, we have focused this Deception Detection example on the provenance of the walk-in document that catalyzed the case. The same process, however, could be used to examine the possibility of deception surrounding any of the actors or evidence in the case.

Task 2.

Use Deception Detection to determine whether deception may be occurring in the case of Wen Ho Lee.

Step 1: Using Table 4.3 in the book as your guide, determine whether Deception Detection should be conducted. Assuming that the United States and the FBI would be the target, who would be the most likely perpetrators of deception? If a case can be made that someone may have a motive to deceive, state this as a hypothesis to be proved or disproved. Note which indicators best apply to this case. Table 4.6 shows a sample response.

Table 4.6 ▶ When to Use Deception Detection: The Wen Ho Lee Case

Analysts should be concerned about the possibility of deception when:	Information suggesting indicators may be true:
The potential deceiver has a history of conducting deception.	China has a long-standing tradition of deploying deception.
Key information is received at a critical time, that is, when either the recipient or the potential deceiver has a great deal to gain or to lose.	China could have planted the walk-in to throw the United States off the scent of a more valued intelligence source. It probably knew an investigation was underway.
Information is received from a source whose bona fides are questionable.	The FBI and the CIA questioned the bona fides of the walk-in.
Analysis hinges on a single critical piece of information or reporting.	The W-88 sketch was viewed as a critical piece of evidence by Notra Trulock.

(Continued)

Table 4.6 ▶ When to Use Deception Detection: The Wen Ho Lee Case *(Continued)*

Analysts should be concerned about the possibility of deception when:	Information suggesting indicators may be true:
Accepting new information would require the analyst to alter a key assumption or key judgment.	Analysts may have assumed prior to the walk-in that the Chinese could have received help from the Russians or could have developed the warhead on their own. The walk-in information would lead them to consider an espionage hypothesis more seriously.
Accepting the new information would cause the Intelligence Community, the US government, or the client to expend or divert significant resources.	The walk-in information prompted both the Department of Energy and the FBI to expend substantial resources investigating LANL and Wen Ho Lee.
The potential deceiver may have a feedback channel that illuminates whether and how the deception information is being processed and to what effect.	The Chinese almost certainly have other sources at DOE and the National Labs—or people in contact with employees there—who could report that an investigation was underway.

Step 2: Consider Motive, Opportunity, and Means; Past Opposition Practices; Manipulability of Sources; and Evaluation of Evidence for the potential deceiver. Use the templates and questions in Table 4.4 in the book as your guide. Table 4.7 shows an example response.

When discussing Past Opposition Practices (POP), the question sometimes arises as to whether others besides the Chinese should be considered adversaries. For example, could the adversary be the Taiwanese or Wen Ho Lee himself? It is a good question and should prompt a useful discussion. The fact that such questions arise demonstrates the value of using structured techniques, which help the analyst think critically about the issue, sometimes outside the context of the specific question at hand.

Analytic Value Added: Summarize the results of all four matrices in terms of whether they tend to prove or disprove the deception hypothesis. Did the technique expose any embedded assumptions or critical gaps that need to be examined more critically?

Task 3.

Assess whether the overall potential for deception is an insignificant threat, a possibility but one with no significant policy or resource implications, or a serious concern that merits attention and warrants further investigation.

A relatively strong case can be made here to consider the possibility of a deception operation. Further investigation is warranted, and any final analysis should await the outcome of that investigation.

TECHNIQUE 3: PREMORTEM ANALYSIS AND STRUCTURED SELF-CRITIQUE

The goals of these techniques[1] is to challenge—actively and explicitly—an established mental model or analytic consensus

Table 4.7 ▶ Wen Ho Lee Deception Detection Example

	Motive, Opportunity, and Means (MOM)
Motive: What are the goals and motives of the potential deceiver?	▶ To protect a real or more productive spy by casting suspicion on someone else, namely Wen Ho Lee. ▶ To get rid of Wen Ho Lee if he was becoming a troublesome source. ▶ To confuse any investigation while continuing to procure valuable intelligence.
Channels: What means are available to the potential deceiver to feed information to us?	▶ Double agents feeding information to a known intelligence organization such as the FBI or the CIA. ▶ Providing the US government with "authentic" documentation through a walk-in, for example, a report with drawings that contained more than public information. ▶ Participating in routine scientific exchanges with national lab personnel.
Risks: What consequences would the adversary suffer if such a deception were revealed?	▶ Possible loss of scientific exchanges. ▶ The discovery of informant networks in labs. ▶ The "real" source becoming frightened and no longer cooperating.

Table 4.7 ▶ (*Continued*)

Costs: Would the potential deceiver need to sacrifice sensitive information to establish the credibility of the deception channel?	▶ Not really—much information publicly available. ▶ Engineering "flaws" in document could be deliberate.
Feedback: Does the potential deceiver have a feedback mechanism to monitor the impact of the deception operation?	▶ Scientific delegations making inquiries. ▶ Social conversation with lab personnel. ▶ Wen Ho Lee himself. ▶ Other sources throughout the scientific community and working in the national labs and the US government.
	Past Opposition Practices (POP)
Does the adversary have a history of engaging in deception?	▶ Classic Chinese military doctrine espouses deception.
Does the current circumstance fit the pattern of past deceptions?	▶ China has history of recruiting ethnic Chinese to give it information inadvertently or by revealing unclassified information that, when added up, yields valuable insights but does not provide grounds for a prosecution.
If not, are there other historical precedents?	▶ The entire system of Chinese intelligence gathering offers deniability or the option of casting suspicion on multiple actors.
If not, are there changed circumstances that would explain the use of this form of deception at this time?	
	Manipulability of Sources (MOSES)
Is the source vulnerable to control or manipulation by the potential deceiver?	▶ No information about the source's background; not a recruited asset. ▶ The walk-in probably has relatives on the mainland.
What is the basis for judging the source to be reliable?	▶ Only basis is the actual documentation provided, but that could be part of the deception operation.
Does the source have direct access or only indirect access to the information?	▶ Little information about the access or background of the source; not a recruited source.
How good is the source's track record of reporting?	▶ Source is a walk-in and has no previous track record.
Does the source have personal reasons for providing faulty information, for example, to please the collector, promote a personal agenda, or gain more revenue? Or could a well-meaning source just be naïve?	▶ Unlikely the source would be trying to please the collector or obtain more revenue because there is no established relationship between the source and the collector; it is feasible, however, that the source may have been promoting a personal agenda.
	Evaluation of Evidence (EVE)
How accurate is the source's reporting? Has the whole chain of evidence, including translations, been checked?	▶ Shows a high level of detail but not entirely consistent with what we know Wen Ho Lee to have worked on. ▶ Care was taken to translate the documents well; the sketches speak for themselves.
Does the critical evidence check out? Remember, the subsource can be more critical than the source.	▶ The sketches could be authentic; they reveal a convincing level of detail.
Does evidence from one source of reporting (e.g., human intelligence) conflict with that coming from another source (e.g., signals intelligence or open source reporting)?	▶ No other sources of information to collaborate what was provided by the walk-in. No conflicts but also no independent collaboration.
Do other sources of information provide corroborating evidence?	▶ No other sources of information to collaborate what was provided by the walk-in. No conflicts but also no independent collaboration.

in order to broaden the range of possible explanations or estimates that are seriously considered. This process helps reduce the risk of analytic failure by identifying and analyzing the features of a potential failure before it occurs.

Task 4.

Conduct a Premortem Analysis and Structured Self-Critique of the reigning view in the case study that Wen Ho Lee passed nuclear secrets to the People's Republic of China.

Step 1: Imagine that a period of time has passed since you concluded that Wen Ho Lee was guilty of espionage. You suddenly learn from an unimpeachable source that the judgment was wrong. Then imagine what could have happened to cause the analysis to be wrong.

The first two steps comprise the Premortem Analysis. This right-brain-led, creative brainstorming process asks analysts to imagine a future in which they have been proved wrong and work backward to try to identify the possible causes. In essence, they are identifying the weak links in their analysis in order to avoid these potential pitfalls prior to publishing the analysis or, in this case, bringing a case to prosecution. Most analysts are more left brained than right brained, which often makes imagination techniques like brainstorming challenging. However, when coupled with the Structured Self-Critique, the systematic, left-brained checklist that comprises steps three through eight, brainstorming can be the first step toward identifying sometimes fatal analytic flaws. It is important to encourage students to be as creative as possible when brainstorming, keeping all ideas in play.

In this case, a brainstorming session might prompt students to consider the following:

- Was Wen Ho Lee's behavior any different than that of his colleagues? For example, were his security indiscretions atypical, or did his colleagues often act in the same way, forgetting to report meetings or revealing controlled but not classified information to foreign nationals without permission?
- Was it suspicious or insignificant that Wen Ho Lee entered the lab at 3:30 a.m. Christmas Eve? Was he a Christian who celebrated Christmas? Did he and his colleagues often work late hours?
- Was Wen Ho Lee a member of a broader network that was exploited by Chinese intelligence but did not provide any actual secret information to the Chinese? If so, who else might be in this network? Who else attended the conferences in China along with Wen Ho Lee?

Step 2: Use a brainstorming technique to identify alternative hypotheses that might explain Wen Ho Lee's pattern of behavior. Keep track of these hypotheses.

In this case, students might identify a number of alternative explanations that could be consistent with Wen Ho Lee's known activities. They could include alternative hypotheses that Wen Ho Lee was:

- Simply a sloppy scientist, just like his peers at the lab who often overlook security regulations because they are too focused on their research.
- Part of a "soft spy" network that provided unclassified information to the Chinese but never engaged in espionage.
- Afraid of losing his job and wanting to retain access to files that documented his research activities should they prove useful in a new job.
- Dutifully archiving records as instructed and had to move the files from a classified to an unclassified system because the classified system did not have any tape.
- Actually a double agent that US intelligence was running against the Chinese and could not, for counterintelligence purposes, tell others within the analytic or law enforcement community.

The alternatives should not include scenarios that obviously contradict known facts in the case. Instructors may advise students that some facts, such as the movement of large quantities of information from a classified to an unclassified computer and the presence of job application letters that were drafted but not sent, should be accepted as accurate for the purposes of the case study. As a result, any alternative hypothesis that Wen Ho Lee was conducting industrial espionage for a company that recently hired him would be discarded.

Step 3: Identify key assumptions underlying the consensus view that Wen Ho Lee was guilty of passing nuclear secrets to the Chinese. Could any of these be unsubstantiated? Do some assumptions need caveats? If some are not valid, how much could this affect the analysis?

The most important aspect of this step is the conversation it produces about the effect of assumptions on analysts' confidence level in the mainline judgment itself.

In this case, when assumptions are explicated in this manner, it becomes apparent that some of the key assumptions are unsupported by evidence or have caveats. This lack of evidence suggests that analysts should be prepared to track down additional information, consider alternative explanations, and potentially add caveats to or revise the mainline judgment.

Some key assumptions and notional assessments are listed in Table 4.8.

Table 4.8 ▶ Wen Ho Lee Key Assumptions Check Example

Key Assumption	Assessment
China is developing good access to US scientists.	**Supported.** In the post–Cold War environment, the United States was emphasizing the value of developing strategic partnerships with former adversaries.
China had an aggressive program to collect information from US scientists, targeting Chinese Americans in particular.	**Supported.** The Chinese have developed an extensive network of scientific colleagues, informants, and sources to gather data both openly and covertly.
A Taiwanese American would spy for China.	**With caveats.** Taiwan and China are rivals, and which country to spy for would be influenced by past loyalties and where one's close relatives resided.
Wen Ho Lee passed secret information.	**With caveats.** The information was not classified at the time; it was marked "Protect as Restricted Data." Only later did investigators decide that some of the information was classified.
Wen Ho Lee is the spy.	**Unsupported.** Lee did not have access to the actual information allegedly passed. In fact, the information included revisions made to the design after he lost access to it.
China could have made rapid advances only with the help of stolen secrets; the Chinese could not have pieced together information from open sources or through sanctioned scientific contacts.	**Unsupported.** Almost all the information was in the public domain. The Chinese design was nearly, but not exactly, the same as the US W-88.
The stolen data were unique to Los Alamos Nuclear Laboratory; individuals at other locations were unlikely to have provided the information.	**Unsupported.** The information could have been obtained from other labs. It also could have come from the thirty-six other Chinese employees working in the labs or from Russian scientists.

Step 4: Review the critical evidence that provides the foundation for the argument. Is the analysis based on any critical item of information? On a particular stream of reporting? If any of this evidence or the source of the reporting turned out to be incorrect, how much would this affect the analysis?

In the Wen Ho Lee case, the forensic evidence generated from a review of LANL computer files and Wen Ho Lee's own computer can be assumed to be reliable. Reporting from most other sources is subject to challenge. For example, investigators differed as to whether the information on the tapes was highly sensitive (the "crown jewels") or could be found by searching diligently on the Internet.

Step 5: Is there any contradictory or anomalous information? Was any information overlooked that is inconsistent with the lead hypothesis?

Several key pieces of evidence are inconsistent or at least anomalous with the hypothesis that Wen Ho Lee is a spy, including the following:

- Lee was an informant for the FBI.
- Wen Ho Lee's wife was an informant for the FBI.
- Wen Ho Lee agreed to have his home computer searched.

On the other hand, the fact that Wen Ho Lee did not download computer manuals is inconsistent with the alternative hypothesis that he was only archiving nuclear data he worked on.

Step 6: Is there a potential for deception? Does anyone have motive, opportunity, and means to deceive you, either intentionally or unintentionally?

The available information indicates that the possibility of Chinese deception cannot be discounted. The Chinese certainly had the motive, opportunity, and means to deceive the United States. They also had a deeply rooted tradition of conducting deception operations. Their ability to manipulate the walk-in was restricted because it would have been challenging to maintain communication with the walk-in after he delivered the information. However, the primary value of the walk-in was to provide the initial documentation; the Chinese could have used other channels, including double agents, to continue the deception operation. The quantity of evidence and the level of detail in the evidence provided by the walk-in are

consistent with both hypotheses: that the walk-in was legitimate or that the Chinese decided to provide detailed information to make the walk-in look credible in the eyes of US government officials.

Step 7: Is there an absence of evidence, and does it influence the key judgment? Table 4.9 shows an example response.

Table 4.9 ▶ Wen Ho Lee Absence of Evidence Assessment Example

Absence of Evidence	Assessment
No evidence of Wen Ho Lee ever passing documents to the Chinese.	Although Wen Ho Lee was suspected of providing nuclear secrets to the Chinese, no evidence was ever provided that documents were physically passed.
No evidence that Wen Ho Lee had communicated secrets orally to the Chinese.	The FBI never presented any evidence that Wen Ho Lee provided classified information to the Chinese in any of his meetings or conversations.

Step 8: Have you considered the presence of common analytic pitfalls such as confirmation bias, "satisficing," and historical analogy? (Use Table 1.2 in chapter 1 as your guide to do so.) Table 4.10 shows an example response.

Table 4.10 ▶ Wen Ho Lee Common Analytic Pitfalls Example

Analytic Pitfall	Assessment
Mindset	The mindset that the Chinese could not develop the W-88 without stealing nuclear secrets from the United States. The mindset that LANL and Wen Ho Lee would be the logical source of the leak. But what if this is untrue in this case? Are there alternative hypotheses? Once a mindset is identified, it must be challenged.
Confirmation bias	We tend to see what we expect to see, and we tend to look for evidence that confirms our mindset. In this case, it is easy to accept assumptions masquerading as fact because they conform to our mindset. For example, when Wen Ho Lee withdrew $700 in Hong Kong, analysts observed that this would be enough money to pay for a flight to Shanghai. There was no evidence to suggest that such a flight ever occurred.
"Satisficing"	It is easy to jump to the first, most plausible explanation in the presence of firmly held mindsets. In this case, given the substantial pressure on the FBI to pursue vigorously any reports of Chinese scientific espionage and the existence of a DOE study that nuclear secrets probably were stolen from LANL and most likely by Wen Ho Lee, an FBI investigation of Wen Ho Lee was likely to satisfy most critics.
Historical analogy	In the presence of a long history of Chinese espionage targeting Chinese American scientists in the United States, it is easy to conclude that an investigation of Wen Ho Lee is a priority. This assumes that what has happened before is happening again.

Step 9: Based on the answers to the themes of inquiry outlined, list the potential deficiencies in the argument in order of potential impact on the analysis.

Analysts should recognize that there are potential deficiencies in each element of the Premortem Analysis, including the following:

- Unsupported assumptions.
- Presence of credible alternative hypotheses.
- Absence of evidence.
- Presence of analytic pitfalls.
- Potential for deception.

Analytic Value Added: As a result of your analysis, would you retain, add a caveat to, or dismiss the mainline judgment, and why? Students should seek to add caveats to their analysis in order to reflect the uncertainty introduced by unsupported assumptions, the possibility that alternative hypotheses could explain Wen Ho Lee's behavior, the absence of hard evidence that anything was actually passed to the Chinese, the potential for deception, and the presence of analytic pitfalls. They should also cite the gaps in their information base and consider what would be the most profitable avenues for new research and investigation.

In this case, the case for Wen Ho Lee's guilt is at least as strong as the case for his innocence. Perhaps the more productive strategy would be to focus on which alternative hypotheses are most consistent with his actual behavior and what implications these hypotheses might have for federal investigators. If, for example, the fact that Wen Ho Lee is part of an informal network of informants is deemed credible, then attention should turn to who comprised that

network and whether the other members of the network are doing greater damage to US national security interests than Wen Ho Lee.

In dealing with the potential for deception, it is important to keep in mind that often the issue is not "Was someone being deceptive?" but "Is there sufficient evidence or argumentation to justify opening a major investigation and dedicating significant resources to find out?"

Task 5.

Rewrite the lead judgment of the case so that it reflects any changes you would incorporate as a result of the Premortem Analysis.

CONCLUSION

Wen Ho Lee is retired and living in Albuquerque, New Mexico. At the conclusion of his trial, the presiding judge took the unusual step of issuing an apology from the bench, saying, "I sincerely apologize to you, Dr. Lee, for the unfair manner you were held in custody by the Executive Branch."[2] After the trial concluded, Lee filed a lawsuit against the *Los Angeles Times,* the *Washington Post,* ABC, the Associated Press, and the *New York Times* for invasion of his privacy.[3] He ultimately won the lawsuit. Lee subsequently wrote a book titled *My Country versus Me: The First-Hand Account by the Los Alamos Scientist Who Was Falsely Accused of Being a Spy.* He also completed a textbook on applied physics, which he began writing while he was in prison.[4]

KEY TAKEAWAYS

Application of structured analytic techniques to the Wen Ho Lee case underscores the need to:

- Always challenge inherited assumptions. The Department of Energy presented the FBI with the findings of an administrative inquiry that was based on several key—and unchallenged—assumptions. Before launching the investigation of Wen Ho Lee, it is important to critically examine the key assumptions upon which the DOE case was based.
- Be open to alternative hypotheses. When data are inconsistent with the lead hypothesis, stop and ask yourself if there are alternative and more compelling explanations for the behavior being observed.
- Make time to reflect, especially at the start of a new project or investigation. When operating under major time constraints and substantial pressure from above to produce, avoid the temptation to "plunge in." The need to employ structured analytic techniques, like a Key Assumptions Check, is greatest when the stakes are high. A quick answer will satisfy your customer for the moment, but you will have to live with a wrong answer for the rest of your life.

NOTES

1. The steps as outlined in this case combine the processes for a Premortem Analysis and Structured Self-Critique. This combination is particularly helpful in cases that require analysts to think broadly, imaginatively, and exhaustively about how they might have been wrong. The Premortem Analysis taps into the creative brainstorming process, and the Structured Self-Critique provides a step-by-step assessment of each analytic element. To aid students' learning process, the questions in this case have already been narrowed from the fuller set of Structured Self-Critique questions found in Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, 2nd ed. (Washington, DC: CQ Press, 2015).

2. Matthew Purdy, "The Prosecution Unravels: The Case of Wen Ho Lee," with James Sterngold, *New York Times,* February 5, 2001, http://www.nytimes.com/2001/02/05/us/the-prosecution-unravels-the-case-of-wen-ho-lee.html.

3. Paul Farhi, "US, Media Settle with Wen Ho Lee," *Washington Post,* June 3, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/02/AR2006060201060.html.

4. Wen Ho Lee, *My Country versus Me: The First-Hand Account by the Los Alamos Scientist Who Was Falsely Accused of Being a Spy* (New York: Hyperion Press, 2002); Wen Ho Lee, *Computer Simulation of Shaped Charge Problems* (Hackensack, NJ: World Scientific, 2006).

Table 5.1 ▶ Case Snapshot: Jousting with Cuba over Radio Marti		
Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Chronologies and Timelines	p. 56	Decomposition and Visualization
Deception Detection	p. 198	Hypothesis Generation and Testing
Quadrant Hypothesis Generation	p. 175	Hypothesis Generation and Testing
Analysis of Competing Hypotheses	p. 181	Hypothesis Generation and Testing

5 Jousting with Cuba over Radio Marti
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

The US government jousted with Cuba for four years over radio broadcasts to Cuba from Florida. Cuban president Fidel Castro saw the plan as one more deliberate American challenge to the legitimacy of the Cuban Revolution. Both countries engaged in threats and counterthreats, and the full range of intelligence collection and analysis capabilities was employed, including open source, human, and technical collection efforts. Analysts were called in to help the Reagan administration assess how Castro would respond if Radio Marti started broadcasting.

In this situation, use of Chronologies and Timelines would help analysts evaluate Castro's behavior and determine whether he was prompting the United States to respond to his initiatives or simply reacting to US actions. Part of this process of evaluation involves using the Deception Detection technique to explore whether some of the information or reporting could be deliberate deception meant to intimidate Washington and persuade the US Congress or the executive branch that broadcasts to Cuba would be too risky. Many speculated about what Castro might do, but a technique such as Quadrant Hypothesis Generation would help structure this process, generating a more rigorous set of hypotheses. Use of hypothesis-testing techniques such as Analysis of Competing Hypotheses would help analysts assess which actions Castro would be most likely to take, further illuminating whether events could be leading up to a radio war with Cuba.

TECHNIQUE 1: CHRONOLOGIES AND TIMELINES

Chronologies and Timelines are simple but useful tools that help order events sequentially; display the information graphically; and identify possible gaps, anomalies, or correlations. In addition, these techniques pull the analyst out of the evidentiary weeds to view a data set from a more strategic vantage point. The complex and contradictory data in this case make an annotated Timeline particularly useful in identifying key pieces of evidence, confidence levels in the reporting, and gaps in the information.

Task 1.

Create a Chronology and Timeline of relevant events leading up to President Reagan's decision to sign the Radio Marti legislation on 4 October 1983 (see Table 5.5).

Step 1: Identify all the key events and arrange them chronologically in a table with one column for the date and one column for the event.

Table 5.5 ▶ Chronology of the Radio Marti Case	
1981	Ronald Reagan inaugurated President of the United States on 20 January.
	In August, during technical discussions concerning radio interference, Cuba says it will move forward with plans for two 500 kW stations and shift to frequency 1040 kHz—the frequency designated for Radio Marti in Florida but also used by clear channel station WHO in Iowa.[1]
	On 22 September, US president Reagan announces Executive Order 12323, setting up the Presidential Commission on Broadcasting to Cuba.[2]
1982	The Board of Directors of the Florida Association of Broadcasters adopts a resolution urging the United States to jam Cuban radio broadcasts until illegal interference from Cuba ends.[3]

(Continued)

Table 5.5 ▶ Chronology of the Radio Marti Case *(Continued)*

	The US House of Representatives passes H.R. 5427 on 10 August, authorizing Radio Marti.
	Cuba on 30 August disrupts broadcasts of radio station WHO in Des Moines, Iowa, and several other stations across the United States.
	Committee on Foreign Relations on 9 September approves Radio Marti legislation.
	The US Senate on 21 December declines to take up Radio Marti legislation.
1983	Commercial broadcasters are informed in May that US countermeasures include destruction of offending Cuban transmitters if Cuba interferes with US radio stations.
	Amended version of Radio Marti legislation passes the US Senate on 13 September. Revised legislation requires Radio Marti to adopt Voice of America (VOA) standards and broadcast on 1180 kHz.
	Radio Marti legislation passes the US House of Representatives on 29 September with a legislative history that enables Radio Marti to become a surrogate home broadcasting service for Cuba.
	President Reagan signs the legislation on 4 October.

Step 2: Select the most relevant information from the case narrative. Consider how best to array the data along the Timeline. Can the information be organized by category? Construct a Timeline of the Radio Marti case.

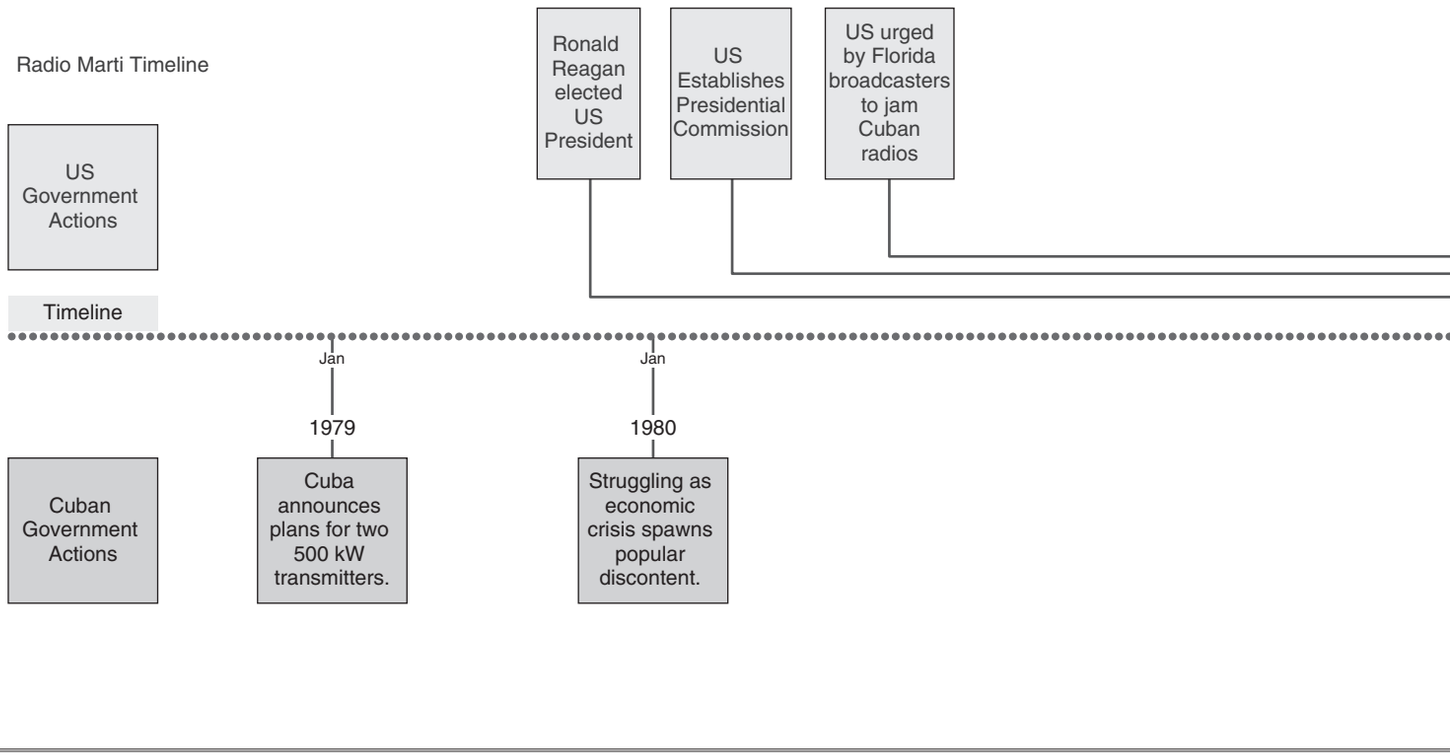
A Timeline that contrasts US actions with Cuban actions is provided in Figure 5.3.

Step 3: Review the Timeline by asking the following questions: Should any underlying assumptions about the evidence be taken into consideration? Do the duration and sequence of events suggested by the data make sense? Are there data gaps? Could any events outside the Timeline have influenced the activities?

A review of the Timeline suggests four major observations:

- The issue was very contentious for the political system in the United States, both in terms of congressional infighting and within the broader population.
- Cuban actions were both proactive and reactive and tended to keep Washington off balance.

Figure 5.3 ▶ Radio Marti: Timeline of US and Cuban Actions



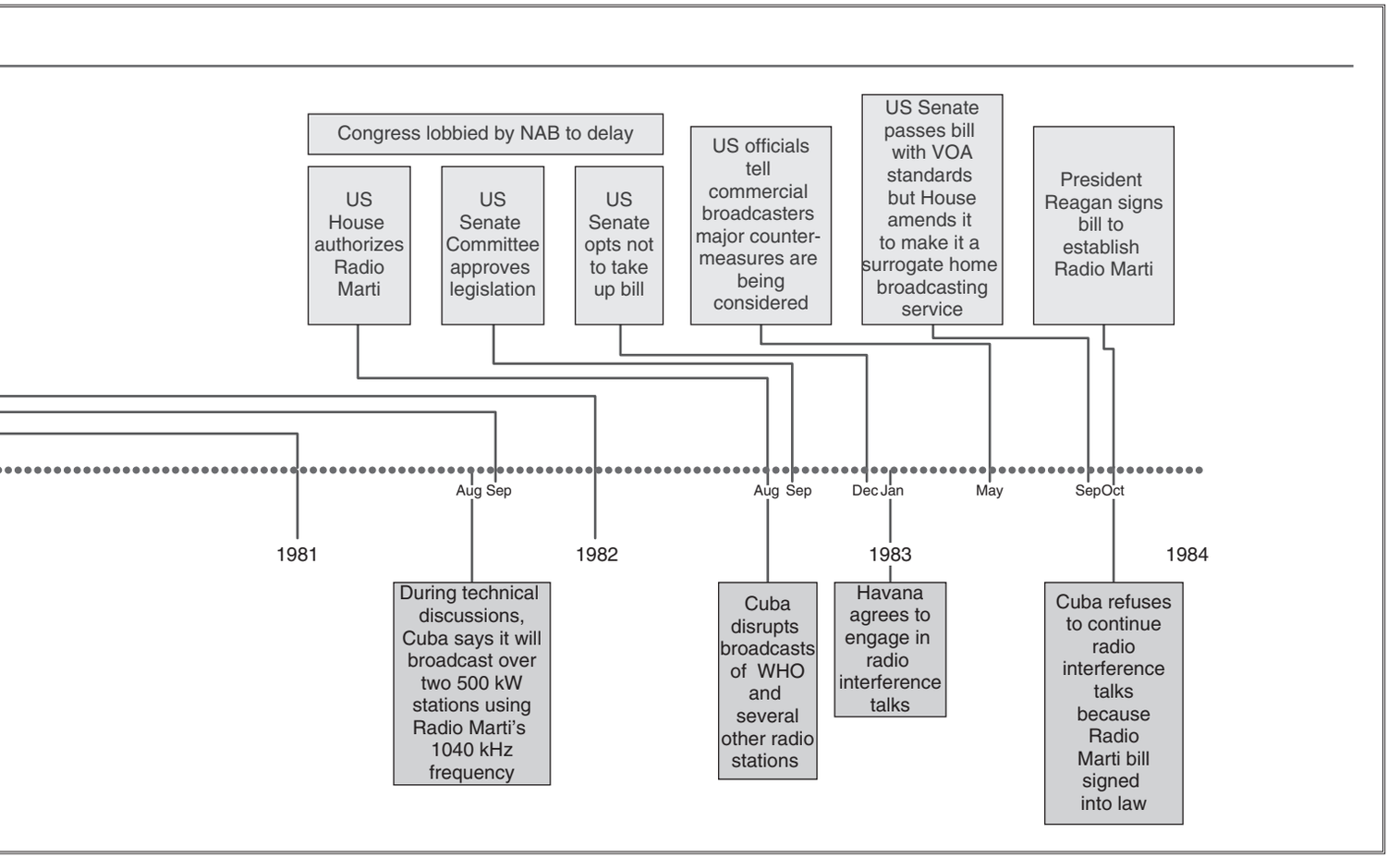
- The launch of Radio Marti probably was delayed by at least one year.
- Castro did not carry out his threat of massive radio interference. We do not know whether it was because he never intended to do so and was transmitting false and deceptive information through public as well as intelligence channels, or, alternatively, that he intended to do so and changed his mind at the last minute for reasons unknown or because he did not want to suffer the costs of US retaliation on this issue.

A major gap in this record is the lack of information from clandestine sources and to what extent this influenced US government actions. Cuba has a long and persistent record of attempting to influence the perceptions of US executive and legislative branch officials. More important, we now know that during this time the Cubans controlled US assets reporting from Cuba and, according to a State Department officer, used them for passing information through intelligence channels. More information about these activities would help in assessing the effectiveness of Cuban perception management/deception efforts.

Analytic Value Added: How confident are you in the sources of information? What does the sequence of events tell you? Are there any gaps in the information that should be addressed? Should you seek any additional information? We would have high confidence in the sources of information on US government actions because they are mostly a matter of public record. Information on Cuban actions is derived from both first- and second-hand sources, which would give us a medium level of confidence. A key gap in the information is what US and Cuban officials were thinking and doing in late 1984 and early 1985 before Radio Marti went on the air.

TECHNIQUE 2: DECEPTION DETECTION

The Radio Marti case presented several significant analytic challenges. One of the principal challenges was whether the Castro regime was engaging in perceptions management and/or strategic deception to support its opposition to Radio Marti. Analysts should routinely consider the possibility that adversaries are attempting to mislead them or to hide important information. The possibility of deception



cannot be rejected simply because there is no evidence of it; if deception is well done, one should not expect to see evidence of it. There are, however, some indicators that should alert analysts that they may be targets of deception, such as the timing of reporting, the bona fides of a source, or when believing what a source says could have known and potentially serious consequences.

Cuba had been engaged in adversarial relations with the United States for two decades before the Reagan administration came into office. Both sides had employed the full range of diplomatic and military tactics, including the threat posed by nuclear missiles on Cuban soil. The Soviet Union and its external intelligence service (the KGB) had mentored and supported the Cuban service. The KGB had a long history of using perceptions management and deception. Given these background circumstances, analysts need to be alert to the possibility that the opposition would employ perceptions management and/or deception to help achieve its goals.

Task 2.

Using Deception Detection techniques, determine whether Cuba might be employing perceptions management and/or deception against the United States.

Step 1: Using Table 5.2 in the book as your guide, assess whether a good case can be made to employ Deception Detection techniques. If a case can be made that Cuba has a motive to deceive, state this as a hypothesis to be proved or disproved.

As discussed in Table 5.6, most Cuba-watchers would say that a strong case could be made that Havana would consider using deception to thwart US efforts to broadcast into Cuba with Radio Marti.

Step 2: One method of structuring analysis to help analysts evaluate their data for possible deception by the opposition can be found in four checklists identified by their acronyms: Motive, Opportunity, and Means (MOM); Past Opposition Practices (POP); Manipulability of Sources (MOSES); and Evaluation of Evidence (EVE). Use the templates and questions in Table 5.3 in the book as your guide.

As noted in Table 5.7, a strong case can be made that the Cuban government employed perceptions management and deception techniques in the case of Radio Marti.

Analytic Value Added: Summarize the results of all four checklists in terms of whether they tend to prove or disprove the deception hypothesis. Did the technique

Table 5.6 ▶ Radio Marti: Likelihood That Cuba Is Employing Deception

Analysts should be concerned about the possibility of deception when:	
The potential deceiver has a history of conducting deception.	The Cuban government—as well as its Soviet ally—has a long history of employing deception.
Key information is received at a critical time—that is, when either the recipient or the potential deceiver has a great deal to gain or to lose.	Cuban threats and actions were often received in response to critical congressional actions on Radio Marti. Both public and private statements suggested that the Cuban government believed it had much to lose if the United States began broadcasting to Cuba. It was concerned that Radio Marti programming would publicize the failures of the revolutionary government and help foment discontent with the regime.
Information is received from a source whose bona fides are questionable.	
Analysis hinges on a single critical piece of information or reporting.	
Accepting new information would require the analyst to alter a key assumption or key judgment.	Accepting reports that Cuba was preparing to jam or otherwise interfere with US radio broadcasting could prompt the US Congress to decide not to initiate broadcasts, anticipating the commotion this might generate in the business community.
Accepting the new information would cause the Intelligence Community, the US government, or the client to expend or divert significant resources.	Accepting reports that Cuba was preparing to jam or otherwise interfere with US radio broadcasting prompted Washington to develop costly countermeasures.
The potential deceiver may have a feedback channel that illuminates whether and how the deceptive information is being processed, and to what effect.	The Cubans had a timely, accurate feedback channel throughout this period in the form of congressional reaction to its various threats and the access to questions about Radio Marti received by its double agents. In addition, its own penetrations of the US government, discovered or undiscovered, may have been able to provide additional reporting.

Table 5.7 ▶ Radio Marti: Assessing the Likelihood of Cuban Deception with MOM, POP, MOSES, and EVE

	Motive, Opportunity, and Means (MOM):
Motive: What are the goals and motives of the potential deceiver?	In the case of Radio Marti, the Cuban goal was clear: prevent Radio Marti from broadcasting to Cuba as a surrogate radio service providing a source of internal news not controlled by the Castro regime. To thwart the US administration's plan, Cuba's best tactic was to prevent passage of the legislation in the US Congress, or cause Congress to modify the broadcast content of Radio Marti so that it would not cause internal problems for the Cuban government. Threats to disrupt US broadcasts if Radio Marti began broadcasting were a tactic designed to encourage opposition of powerful US commercial interests and their representatives in Congress to oppose Radio Marti.
Channels: What means are available to the potential deceiver to feed information to us?	The United States was receiving information about Cuba's intentions through multiple channels. Open sources included public statements by Cuban diplomats and other officials. Diplomatic exchanges in multiple forums provided additional information. Cuba's demonstration of the power of its transmitters to disrupt US broadcasts provided both open information and data for technical analysis of the capabilities of the transmitters. In addition, if Cuba could control some or all of the opposition's clandestine collection of intelligence about Cuban intentions, it could influence US perceptions of its intentions.
Risks: What consequences would the adversary suffer if such a deception were revealed?	Given the Cubans' objective of thwarting the Reagan administration's plans for Radio Marti, if the deception failed or was detected and failed, the worst that could happen would be that Radio Marti would start up, probably sooner rather than later because the administration would not need to prepare countermeasures and would not be running the political risks involved with Cuba disrupting US radio broadcasting. Detection of a deception operation also runs the risk that the opposition will identify the means by which the deception is being conducted. The risk to the Cubans would be calculated in terms of the value of those means.
Costs: Would the potential deceiver need to sacrifice sensitive information to establish the credibility of the deception channel?	Castro's intentions were the critical information in this case. If Castro were providing that information as part of the deception or perceptions management campaign, no sensitive information would be lost and there would be no cost.
Feedback: Does the potential deceiver have a feedback mechanism to monitor the impact of the deception operation?	The Cubans had rich sources of feedback on a potential deception. The response of the main target, the US Congress, and various interest groups provided an excellent means of monitoring the impact of a deception and its continuing credibility. If the Cubans controlled some or all of the clandestine information, they could gain some insights about how the opposition assessed the information and its impact on their analysis by evaluating the follow-up questions asked of their controlled sources.
	Past Opposition Practices (POP):
Does the adversary have a history of engaging in deception?	The clandestine introduction of Soviet nuclear missiles into Cuba represented one of the great strategic deceptions of the 20th century. The Cubans were partners and enablers in that deception.[4]
Does the current circumstance fit the pattern of past deceptions?	Deception is often used by a weak or weaker power against a stronger adversary. In that sense, the possibility of Cuban deception would fit a well-established universal pattern of deception. The specifics of this case indicate that Cuba would have a motive for deceiving the United States about its intentions to disrupt radio broadcasting. However, no specific information was available at the time to indicate whether or not they would disrupt broadcasts.
If not, are there other historical precedents?	The Cuban Missile Crisis provides a robust historical precedent for attempting to deceive the United States.
If not, are there changed circumstances that would explain the use of this form of deception at this time?	The generalized history of deception is the guiding principle in this case.
	Manipulability of Sources (MOSES):
Is the source vulnerable to control or manipulation by the potential deceiver?	The Cubans had the potential to manipulate all of the open sources providing information about their position on Radio Marti. Furthermore, they had the ability to coordinate their open source information with any controlled clandestine collection.
What is the basis for judging the source to be reliable?	Open sources could be manipulated at will. Technical information derived from open sources would be much more difficult to manipulate. Specifically, the capabilities of the Cuban transmitters to disrupt US radio broadcasts were subject to standard technical analytic techniques. Clandestine human sources can always be manipulated if controlled. In addition to standard counterintelligence tradecraft used to vet sources, the specific sources reporting on Radio Marti could be evaluated, in part, by the consistency of their reporting with other sources of information.

(Continued)

Table 5.7 ▶ Radio Marti: Assessing the Likelihood of Cuban Deception with MOM, POP, MOSES, and EVE *(Continued)*

Does the source have direct access or only indirect access to the information?	In this case, whether sources had direct access to the information or not would not provide the analysts with any means to judge whether Castro knew what he would do at the end of the day, was telling the truth to the source, or was manipulating the source.[5]
How good is the source's track record of reporting?	Even if the source had been reporting for a substantial period of time, the question is whether the source was controlled, and, if so, at what point was he controlled.
Does the source have personal reasons for providing faulty information—for example, to please the collector, promote a personal agenda, or gain more revenue? Or could a well-meaning source just be naive?	Not applicable.
	Evaluation of Evidence (EVE):
How accurate is the source's reporting? Has the whole chain of evidence, including translations, been checked?	In this case, analysts had a substantial body of sources derived from open, clandestine, human, and technical means of collection.
Does the critical evidence check out? Remember, the subsource can be more critical than the source.	The critical unknown was how Fidel Castro would respond when and if Radio Marti began to broadcast to Cuba; that could only be determined at the last minute. The United States would likely learn of that final decision by listening to US radio stations.
Does evidence from one source of reporting (e.g., human intelligence) conflict with that coming from another source (e.g., signals intelligence or open source reporting)?	No. But analytically, this could be a sign of deception. Conflicts and inconsistencies are the norm in intelligence collection.
Is any evidence one would expect to see noteworthy by its absence?	Yes. See above.
Do other sources of information provide corroborating evidence?	No. However, as noted, no evidence could answer the ultimate question—what would Fidel do when he heard Radio Marti in Havana?

expose any embedded assumptions or critical gaps that need to be examined more critically? The analysis contained in all four checklists makes a strong case for the likelihood of deception:

- Cuba had strong motivation to engage in deception. Havana believed Radio Marti broadcasts could quickly fan the flames of popular discontent with the Castro regime, lacked the wherewithal to resist such an initiative with military force or economic sanctions, and dared not give the United States a reason for taking direct action against the island.
- Cuba and its Soviet benefactor both had a strong tradition of conducting deception operations.
- The Cuban regime controlled all public information sources on the island, and—as was learned in later years—it also was manipulating US perceptions through a network of double agents. More important, it had a network of spies that had penetrated much of official Washington as well as Florida, which gave it an excellent feedback loop with which to calibrate any deception operation.
- The lack of open source or classified reporting on Cuban internal dynamics and strategizing makes it harder to make a case for deception based on the Evaluation of Evidence.

The technique exposed several assumptions and gaps in information:

- A key assumption was that Cuba's only strategy for opposing the startup of Radio Marti was to disrupt US commercial AM radio broadcasts. Several other options were available to Havana, including sabotaging the facility, jamming the broadcasts, and terminating bilateral agreements that would do harm to the interests of the Cuban American community.
- Little was known about what Fidel Castro and his core leadership were actually thinking and planning.
- Little also was known about the sophistication of Cuban espionage and perception management operations in the United States.

TECHNIQUE 3: MULTIPLE HYPOTHSIS GENERATION: QUADRANT HYPOTHESIS GENERATION

Many techniques can be used to help generate a set of hypotheses, including basic brainstorming, Simple Hypothesis Generation using the Structured Brainstorming technique, Quadrant Hypothesis Generation using a 2 × 2 matrix to structure the process, and the Multiple Hypotheses Generator™. The Multiple Hypotheses Generator™ is a software tool that applies the journalist's classic set of questions (Who? What? How? When? Where? and Why?) to develop a set of mutually exclusive hypotheses by generating permutations of the lead hypothesis.[6]

Of the four techniques just mentioned, basic brainstorming is the least rigorous because it simply involves listing what first comes to mind. Such an unstructured process usually fails the key test of hypothesis generation: that the set of hypotheses generated should be comprehensive and mutually exclusive. The other three techniques are more likely to pass this test if performed correctly.

In this case study, Quadrant Hypothesis Generation would be a good choice because the analytic challenge can be defined along two key dimensions: what range of options the Cubans might consider and how serious the impact might be on the United States. By creating four mutually exclusive quadrants, each defined by different endpoints of the two key dimensions, the Quadrant Hypothesis Generation process reframes the question in four different ways, spurring more creativity and ensuring a more comprehensive analytic approach.

Task 3.

Use the Quadrant Hypothesis Generation technique to develop a set of three to five hypotheses that address the question: How will Cuba respond to the launch of Radio Marti broadcasts?

Step 1: Identify two key dimensions or drivers influencing Cuba's decision making about how to respond using Structured Brainstorming or drawing from expert analysis.

The two primary actors in this case study are Cuba and the United States. In determining a set of key drivers or key dimensions of the issue, this is the best place to start. With regard to Cuba, the key question is: What is Castro's underlying objective? Is he determined to prevent Radio Marti from broadcasting regardless of the consequences, or would he be satisfied with partial success by delaying the launch date or modifying the programming so that it posed less danger to the regime? From the perspective of the United States, the key concern would be how much damage Cuba intended to inflict on the United States. Would it go so far as to disrupt all US commercial AM broadcasting and even attack Radio Marti facilities in Florida, or would it settle for a milder response by only jamming US broadcasts or even not responding at all?

Step 2: Construct a 2 × 2 matrix using the two drivers or primary dimensions of the issue. Use Figure 5.2 as a template.

Step 3: Think of each key dimension or driver as a continuum from one extreme to another. Write the extremes of each of the drivers at the end of the vertical and horizontal axes.

In this instance, the two key dimensions would be **Cuban Objectives** in trying to counter US broadcasting to Cuba on Radio Marti and the potential **Impact on the United States** of any Cuban actions. In terms of Cuban Objectives, the extremes would be either to **Prevent** any US broadcasting by Radio Marti or, at the other end of the spectrum, to accept a more moderate response by seeking to **Delay or Modify** the content of the broadcasts, as shown in Figure 5.4.

Step 4: In each quadrant, describe a likely endstate that would be shaped by the two dimensions or drivers. Some quadrants may have more than one endstate defined.

Potential endstates are described below for each quadrant (see Table 5.8) and summarized graphically in Figure 5.5.

The following two steps (5 and 6) form part of the technique but will not be used in this case study:

Step 5: Develop signposts or indicators that show whether developments are moving toward one of the endstates.

Step 6: Use the signposts to develop intelligence collection strategies to determine the direction in which events are moving.

Analytic Value Added: Did the Quadrant Hypothesis Generation technique help you generate alternative hypotheses that you might not have thought of using traditional brainstorming techniques? Was your resulting set of hypotheses mutually exclusive and

Figure 5.4 Radio Marti: Quadrant Hypothesis Drivers

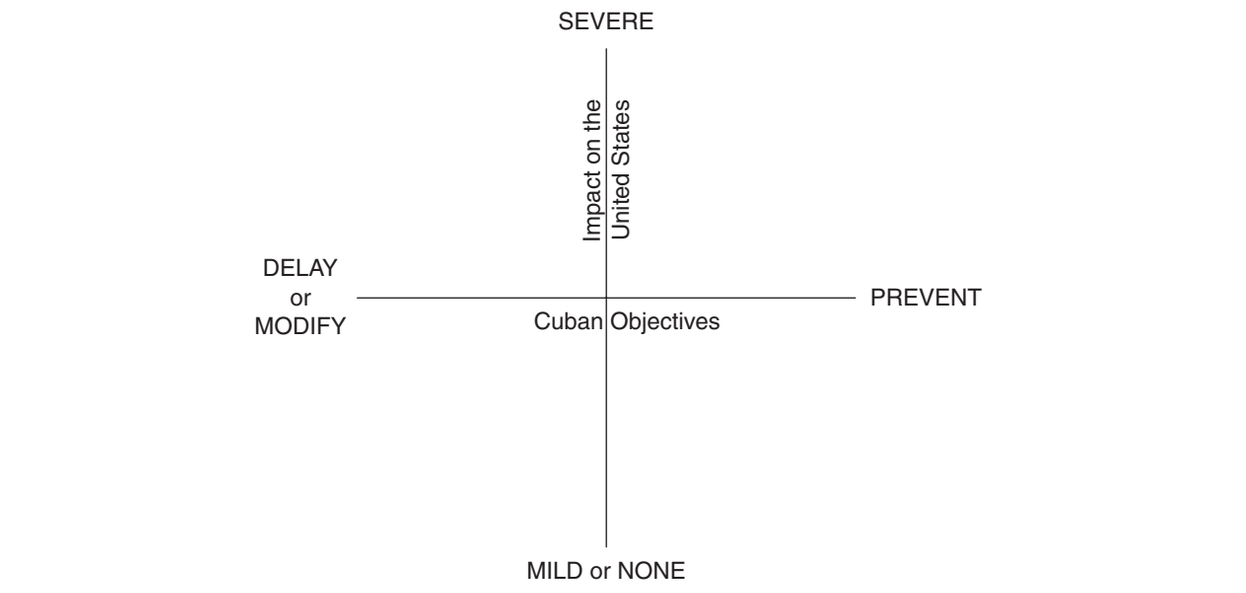
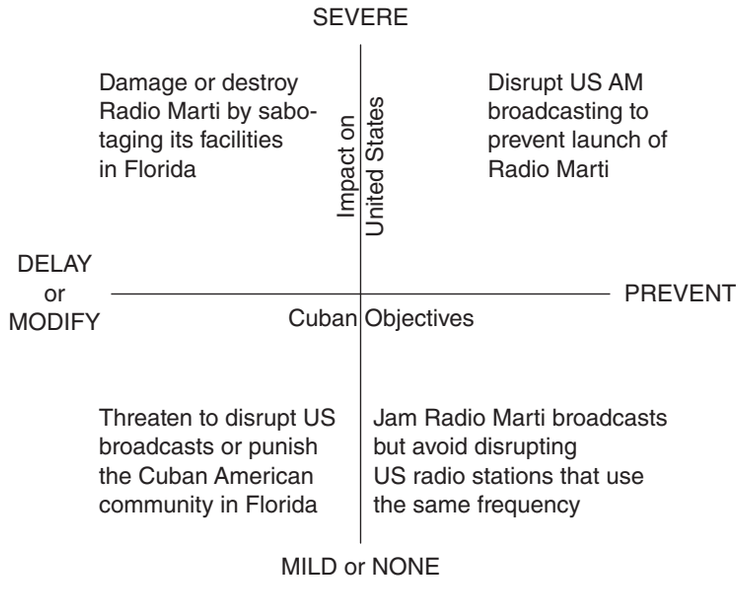


Table 5.8 ▶ Radio Marti: Quadrant Hypotheses Generation Endstates

Hypothesis	Description	Comment
1. Prevent Radio Marti broadcasts in a way that would have **Severe Impact** on the United States	Use threats and then proceed to disrupt US radio broadcasting across most, if not all, of the United States to force the US administration to shut down Radio Marti.	The Cubans have demonstrated the capability to disrupt US radio broadcasts and could do so indefinitely or until the United States agreed to shut down Radio Marti. The Cubans, however, would be risking US retaliation.
2. Delay or Modify Radio Marti broadcasts in a way that would have **Severe Impact** on the United States	Damage or destroy Radio Marti broadcast facilities, especially the antennas in Florida, to delay—or repeatedly delay—its broadcasts.	The Cubans have, or could develop, a clandestine infrastructure in Florida to damage the Radio Marti transmitters on Marathon Key. This highly risky response would more likely delay rather than end Radio Marti broadcasts.
3. Prevent Radio Marti broadcasts in a way that would have **Mild or No Impact** on the United States	Jam Radio Marti broadcasts but do not use sufficient power to interfere with US commercial broadcasting and do nothing else.	Jamming is a traditional response to unwelcome foreign radio broadcasts, widely employed by the Soviet Union and other Communist states. The challenge for Cuba would be to jam the signal but avoid disrupting US broadcasts using the same frequencies.
4a. Delay or Modify Radio Marti broadcasts in a way that would have **Mild or No Impact** on the United States	Threaten to disrupt US radio broadcasts and conduct some disruption as a bluff to deter the United States from initiating broadcasts, but do not actually engage in disruption if Radio Marti starts broadcasting.	With the transmitters in place, Cuba would incur little incremental cost to threaten to use them to disrupt US broadcasts as a ploy to prevent or delay Radio Marti broadcasts. However, if the United States chose to begin broadcasting, the Cubans might calculate the risk of US reprisals would outweigh any benefits from actually disrupting US AM broadcasts.
4b. Delay or Modify Radio Marti broadcasts in a way that would have **Mild or No Impact** on the United States	Threaten to disrupt US radio broadcasts and conduct some disruption as a bluff to cause the United States to modify the content of Radio Marti programming to conform to VOA standards more acceptable to Havana.	Threatened disruption designed to cause changes in content would be more politically palatable in Washington and more likely to succeed.
4c. Delay or Modify Radio Marti broadcasts in a way that would have **Mild or No Impact** on the United States	Take actions to negatively affect the interests of Radio Marti's main proponent, the Cuban American community, by not allowing family members to visit the island or permit their relatives to leave Cuba.	If the Cubans believe that Radio Marti will continue broadcasting and will not change its content, they could try to punish the Cuban American community for supporting Radio Marti.

Figure 5.5 Radio Marti: Quadrant Hypotheses Generation Endstates



comprehensive? Did you generate more than one hypothesis or endstate for any of the quadrants? The Quadrant Hypothesis Generation technique drives the analyst to think about potential hypotheses from four different perspectives. This not only prompts analysts to generate a broader set of hypotheses but also to explore possibilities they would not have otherwise considered. Another advantage is that each quadrant in the 2 × 2 matrix is defined by a different set of drivers or dimensions, thus ensuring that most, if not all, of the hypotheses are mutually exclusive. Obviously, this rule does not hold if two hypotheses are generated for a single quadrant of the 2 × 2 matrix.

This raises a legitimate question as to whether more than one hypothesis should be entered into any quadrant. The argument for a "one hypothesis per quadrant" rule is that this ensures mutual exclusivity. The argument for allowing more than one hypothesis per quadrant is that it spurs analysts to get out of the box and generate a more robust set of hypotheses—some of which often are counterintuitive—and in that sense highly valuable.

In this case study, three hypotheses were generated for the **Delay or Modify** Radio Marti broadcasting with **Modest or No Impact** on the United States. The value in generating more than one hypothesis for this category is that it sparked some new ideas on what actions Havana might undertake—one of which actually came to pass when Cuba terminated the US–Cuba Emigration Agreement, thereby cancelling provisions for Cuban American families to visit their relatives in Cuba.

TECHNIQUE 4: ANALYSIS OF COMPETING HYPOTHESES

The principles of social science research and decades of experiments on cognition and decision making have established that analysts considering complex issues benefit from structuring their analytic process in order to ensure that all relevant data are collected and evaluated as objectively as possible.[7] Analysts face a perennial challenge of working with incomplete, ambiguous, anomalous, and sometimes deceptive data. In addition, strict time constraints on analysis and the need to "make a call" often conspire with a number of natural human cognitive tendencies to result in inaccurate or incomplete judgments.

One approach to structured analysis, Analysis of Competing Hypotheses (ACH), was developed for the Intelligence Community and, particularly, for analysts working on issues in which deception may be employed. ACH improves the analyst's chances of overcoming these challenges by requiring the analyst to identify and refute possible hypotheses using the full range of data, assumptions, and gaps that are pertinent to the problem at hand. According to Heuer and Pherson, "ACH involves identifying a set of mutually exclusive alternative explanations or outcomes (presented as hypotheses), and selecting the hypothesis that best fits the evidence."[8]

Task 4.

Use the ACH software to identify which hypotheses provide the most credible explanation in answering this question: How will Cuba seek to delay or prevent Radio Marti from broadcasting? The basic ACH software is available at http://www.globalytica.com or from the Palo Alto Research Center at http://www2.parc.com. A collaborative version of ACH called Te@mACH® can be accessed at http://www.globalytica.com.

Step 1: Select three to five hypotheses based on the results of Quadrant Hypothesis Generation exercise, striving for mutual exclusivity.

The principal concern of the US stakeholders was that Cuba would disrupt commercial radio broadcasts across the country. However, posing the intelligence question in a broader form, "How will Cuba seek to delay or prevent Radio Marti from broadcasting?" includes other possible responses by the Cubans. So the first step in structuring the analysis is to pose the question properly to ensure that the full range of possible outcomes is considered.

A hypothesis is essentially a person's best guess to answer a question. According to Heuer and Pherson, in an ACH exercise, "Hypotheses should be mutually exclusive; that is, if one hypothesis is true, all others must be false. The list of hypotheses should include all reasonable possibilities. Include a deception hypothesis if that is appropriate."[9] In the case of hypotheses related to Radio Marti, some of the hypotheses would be mutually exclusive only because of the intent of the Cubans, not their capabilities to disrupt US broadcasts. A set of hypotheses to consider is provided in Table 5.9.

Table 5.9 ▶ Radio Marti: Selected Hypotheses for ACH Analysis

No.	Hypothesis
1.	Cuba **Disrupts** US radio broadcasting to prevent Radio Marti broadcasts
2.	Cuba **Sabotages** Radio Marti facilities to delay or prevent Radio Marti broadcasts
3.	Cuba **Jams** Radio Marti broadcasts without disrupting US broadcasts and does nothing else
4.	Cuba **Deceives** with threats and some disruption to delay or modify Radio Marti broadcasts
5.	Cuba **Punishes** the Cuban American community to delay or modify Radio Marti broadcasts

Step 2: Make a list of all relevant information, including significant evidence, arguments, gaps, and assumptions.

See Table 5.10, which identifies fourteen distinct items of relevant information.

Step 3: Assess the relevant information against each hypothesis by asking, "Is this information highly consistent, consistent, highly inconsistent, inconsistent, neutral, or not applicable vis-à-vis the hypothesis?" (The Te@mACH® software does not include the "neutral" category.)

The five hypotheses and fourteen items of relevant information can be entered into the Te@mACH® software tool, and each cell can be rated as shown in Figure 5.6.

Step 4: Refine the matrix by reconsidering the hypotheses. Does it make sense to combine two hypotheses, add a new hypothesis, or disaggregate an existing one?

The **Deceive** and the **Punish** hypotheses might be combined because they seek similar goals—to delay or modify the content of Radio Marti broadcasts—and would risk less retaliation against Cuba by the United States.

Step 5: Draw tentative conclusions about the relative likelihood of each hypothesis. An inconsistency score will be calculated by the software; the hypothesis with the lowest inconsistency score is tentatively the most likely hypothesis. The one with the most inconsistencies is the least likely. The hypotheses with the lowest inconsistency scores appear on the left of the matrix, and those with the highest inconsistency scores appear on the right.

The two hypotheses with the most Inconsistent items of relevant information are the **Sabotage** and **Jam** hypotheses. The **Jam**—and nothing else—hypothesis is inconsistent with much of Cuba's past behavior; it would be highly unlikely for Cuba to decide to stop pressing the US administration to stand down on launching Radio Marti. The **Sabotage** hypothesis had a large number of ratings showing that past Cuban activity to build transmitters and develop a capacity to disrupt broadcasts was inconsistent with a sabotage strategy. Implementing either strategy would not require Cuba to construct a major radio broadcasting capability or demonstrate its ability to disrupt US radio broadcasts.

Two hypotheses—**Disrupt** US radio broadcasting and **Punish** the Cuban American community—had a smaller number of Inconsistent ratings, none of which were compelling, suggesting that they should not be discarded. The

Table 5.10 ▶ Radio Marti: Relevant Information for ACH Analysis

1.	Despite Cuba's signing of the North American Radio Broadcasting (NARB) Agreement in 1950, Cuban interference on the AM band begins to grow in the 1960s after Castro comes to power; by the 1970s, it is a serious problem.
2.	In 1979, Cuba submits an inventory to ITU that includes plans for two radio stations transmitting with 500 kW of power—a volume ten times the limit permitted to any US radio station.
3.	The collapse of the Soviet Union and its economic subsidies severely damages the Cuban economy, resulting in an explosion of popular discontent.
4.	In August 1981, Cuba says it intends to shift the frequencies of its 500 kW stations to 1040 kHz and 1160 kHz.
5.	In 1982, the Board of Directors of the Florida Association of Broadcasters adopts a resolution urging the United States to jam Cuban radio broadcasts until illegal interference from Cuba ends.
6.	Technical intelligence sources confirm the location of the Cuban broadcasting stations.
7.	The Federal Communications Commission (FCC) estimates that, at full power, the two 500 kW transmitters could be heard as far away as Alaska and Hawaii.
8.	On 30 August, the Cuban transmitter broadcasts on 1040 kHz for several hours at 150 kW (three times the US legal maximum), causing significant interference with WHO's broadcasting and several other US radio stations.
9.	The National Association of Broadcasters, citing the broadcasts, lobbies Congress on behalf of farmers and truckers to delay implementation of Radio Marti, and the Senate decides not to take up the legislation.
10.	The *New York Times* reports in May 1983 that senior US officials have told commercial broadcasters that a list of some forty US countermeasures are being considered if Cuba interferes with US radio stations, including destruction of offending Cuban transmitters.
11.	An amended version of Radio Marti legislation passes the US House of Representatives, stating that Radio Marti must adopt Voice of America (VOA) standards.
12.	Congress finally passes Radio Marti legislation in September 1983, with a legislative history that enables Radio Marti to become a surrogate home broadcasting service for Cuba.
13.	The president signs legislation establishing Radio Marti on 4 October 1983.
14.	Radio Marti is set to broadcast from Florida at 50 kW on 1040 kHz, which will not interfere with the signal of radio station WHO in Des Moines, Iowa.

most likely hypothesis to emerge from the analysis was the **Deceive** hypothesis, which had only two Inconsistent ratings.

Step 6: Analyze the sensitivity of your tentative conclusion to a change in the interpretation of a few critical items of information. If using the basic ACH software, sort the evidence by diagnosticity, and the most diagnostic information will appear at the top of the matrix. The Te@mACH® software will automatically display the most diagnostic information at the top of the matrix.

The analysis would be most sensitive to any credible reporting on what Castro and his key advisors were actually thinking or intending to do as the confrontation played out. Discriminating between whether an observed action is intended to manage US perceptions or signal true intent to retaliate is difficult, if not impossible, lacking any information on or access to the actual decision-making process. The value of ACH, in part, is that it helps the analyst think through all possible strategies in a rigorous manner, thereby increasing the analyst's confidence in his or her ability to defend a final judgment.

Step 7: Report the conclusions by considering the relative likelihood of all the hypotheses.

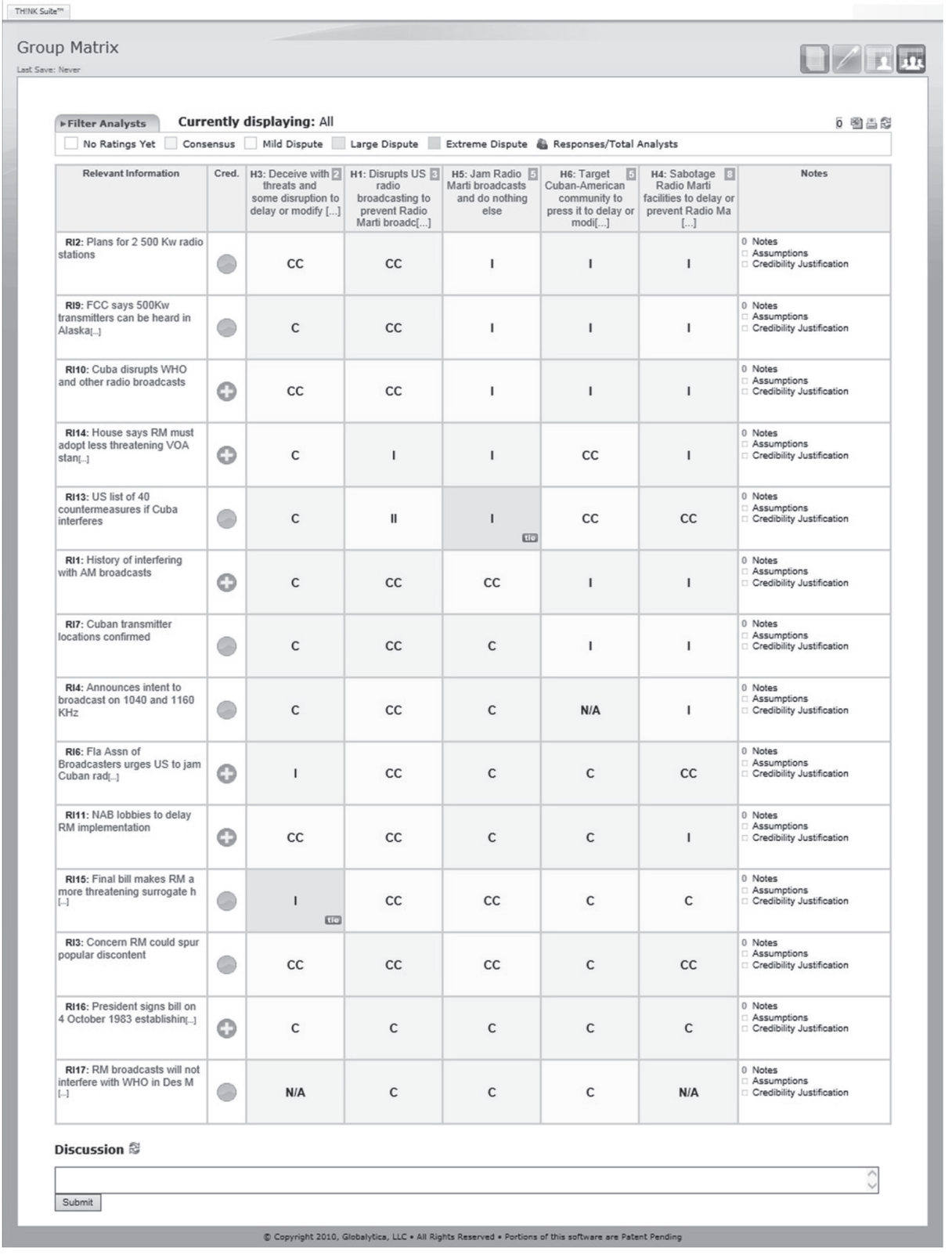
In this case, the **Deceive** hypotheses appear to emerge as Castro's most likely course of action, but caveats would be required. For example, it would be prudent to note that Castro has been known to act precipitously in the past if sufficiently provoked (as he did in shooting down the US U-2 aircraft during the Cuban Missile Crisis).

Step 8: Identify indicators or milestones for future observation.

A good analyst would be on the lookout for information that was inconsistent with any of the lead hypotheses. For example, key indicators to seek that would disprove the **Deceive** hypothesis would include:

- Renewed Cuban efforts to disrupt US commercial broadcasting

Figure 5.6 ▶ Radio Marti: Te@mACH® Group Matrix with Ratings



THINK Suite™

Group Matrix

Last Save: Never

▸Filter Analysts **Currently displaying:** All

No Ratings Yet | Consensus | Mild Dispute | Large Dispute | Extreme Dispute | Responses/Total Analysts

Relevant Information	Cred.	H3: Deceive with threats and some disruption to delay or modify [...] (2)	H1: Disrupts US radio broadcasting to prevent Radio Marti broadc[...] (3)	H5: Jam Radio Marti broadcasts and do nothing else (5)	H6: Target Cuban-American community to press it to delay or modi[...] (5)	H4: Sabotage Radio Marti facilities to delay or prevent Radio Ma [...] (8)	Notes
RI2: Plans for 2 500 Kw radio stations		CC	CC	I	I	I	0 Notes Assumptions Credibility Justification
RI9: FCC says 500Kw transmitters can be heard in Alaska[...]		C	CC	I	I	I	0 Notes Assumptions Credibility Justification
RI10: Cuba disrupts WHO and other radio broadcasts		CC	CC	I	I	I	0 Notes Assumptions Credibility Justification
RI14: House says RM must adopt less threatening VOA stan[...]		C	I	I	CC	I	0 Notes Assumptions Credibility Justification
RI13: US list of 40 countermeasures if Cuba interferes		C	II	I (tie)	CC	CC	0 Notes Assumptions Credibility Justification
RI1: History of interfering with AM broadcasts		C	CC	CC	I	I	0 Notes Assumptions Credibility Justification
RI7: Cuban transmitter locations confirmed		C	CC	C	I	I	0 Notes Assumptions Credibility Justification
RI4: Announces intent to broadcast on 1040 and 1160 KHz		C	CC	C	N/A	I	0 Notes Assumptions Credibility Justification
RI6: Fla Assn of Broadcasters urges US to jam Cuban rad[...]		I	CC	C	C	CC	0 Notes Assumptions Credibility Justification
RI11: NAB lobbies to delay RM implementation		CC	CC	C	C	I	0 Notes Assumptions Credibility Justification
RI15: Final bill makes RM a more threatening surrogate h [...]		I (tie)	CC	CC	C	C	0 Notes Assumptions Credibility Justification
RI3: Concern RM could spur popular discontent		CC	CC	CC	C	CC	0 Notes Assumptions Credibility Justification
RI16: President signs bill on 4 October 1983 establishin[...]		C	C	C	C	C	0 Notes Assumptions Credibility Justification
RI17: RM broadcasts will not interfere with WHO in Des M [...]		N/A	C	C	C	N/A	0 Notes Assumptions Credibility Justification

Discussion

Submit

- A public speech by Castro threatening specific retaliatory action by Cuba
- Reports of Cuban plans to sabotage Radio Marti facilities

Similarly, key indicators that would tend to disprove the **Disrupt** hypothesis that Castro intended to defeat Radio Marti through a program of disrupting US radio broadcasts would include:

- Private assurances from senior Cuban officials to Florida (or other) broadcasters that disruption would not occur
- Relatively moderate statements, made publicly or privately, that Castro was seeking a way to avoid a major confrontation by striking a deal of some sort with the United States

Analytic Value Added: As a result of your analysis, what are the most and least likely hypotheses? What are the most diagnostic items of information? What, if any, assumptions underlie the data? Are there any gaps in the relevant information that could affect your confidence? How confident are you in your assessment of the most likely hypothesis? The analysis suggested that Castro's most likely course of action would be to employ deception and moderate disruption to press the United States to delay or mitigate the effects of Radio Marti by adopting VOA standards. The possibility of taking more serious retaliatory steps, however, could not be ruled out. Much would depend on Castro's state of mind at the time Radio Marti was turned on; his perception of how seriously the United States would retaliate; and his level of confidence that he could jam or otherwise interfere with the signal, making it less politically dangerous for his regime. A key assumption throughout all the analysis is that Castro would act rationally in response to both US and any domestic Cuban stimuli. The biggest gap in information would be Castro's intent. Because so little is known about the intent of Castro—or of any of his key advisors—the level of confidence in the analysis would be medium at best.

CONCLUSION

About two weeks after President Reagan signed the legislation in October 1983 to initiate AM radio broadcasts to Cuba, Havana announced its withdrawal from radio interference talks, citing its opposition to planned broadcasting by Radio Marti to Cuba.[10] Havana also continued to threaten to disrupt US AM commercial radio broadcasting.[11]

Analysts cautioned that regardless of what Castro said publicly—or was predicted to do in intelligence reporting—he could always change his mind at the last minute. From the available facts, analysts could infer that Cuba *could* disrupt US broadcasting, but they could not infer that Cuba *would* disrupt US broadcasting when Radio Marti started broadcasting.

On 20 May 1985, more than a year and a half after the Radio Marti legislation was signed, Radio Marti began broadcasting to Cuba.[12] Cuba did not retaliate by disrupting US commercial AM radio broadcasting. It chose instead to immediately terminate the US–Cuba Emigration Agreement, thereby cancelling provisions for family visits.

VALUE OF USING STRUCTURED ANALYTIC TECHNIQUES

In this case study, the use of Structured Analytic Techniques would have benefited the analytic process in two ways. They would have:

- Encouraged analysts to develop a full range of possible outcomes—or testable hypotheses—including a deception hypothesis. In this situation, the analysts focused mostly on only two outcomes—significant disruption or no significant disruption. To this extent, Skoug was correct when he observed that no one had thought about Cuba striking back at the Cuban American supporters of Radio Marti by cancelling the family visit agreement. By encouraging the development of the full range of hypotheses, Structured Analytic Techniques would have helped analysts inform policy makers about alternative possible outcomes, spurring them in turn to seek more information about those outcomes.
- Prompted analysts to focus on the data most critical in examining which course of action Castro was most likely to take. The use of analytic techniques could have spurred analysts to examine clandestine reporting with special care because it offered the best insights into Castro's true intentions. However, the analysts would have been extremely unlikely to have recognized at the time that Castro controlled virtually all human sources reporting on Cuba collected by the US Intelligence Community and was using that stream of reporting to transmit deceptive information about his plans to respond to Radio

Marti. That said, after Castro did not disrupt US AM broadcasting, some hard questions about the reliability of the key sources could have been asked.[13]

KEY TAKEAWAYS

- Structured analytic techniques provides one of the best mechanisms for overcoming—or, at least, mitigating the effects of—cognitive traps and mental mindsets that lead to making poor analytic judgments. Always develop a full range of credible hypotheses when beginning an analysis. This also helps ensure that policy makers will not be surprised by what actually transpires.
- When working with reporting—particularly from clandestine sources—that is critical to the analysis, always ask if the reporting might be intentionally deceptive. In this case, it was used to reinforce open source reporting that Cuba had the means and the intent to disrupt US AM broadcasting.

NOTES

1. Kenneth N. Skoug Jr., *The United States and Cuba Under Reagan and Shultz: A Foreign Service Officer Reports* (Westport, CT: Praeger, 1996), 17.
2. *E.O. 12323. The Federal Register*.
3. Skoug, *The United States and Cuba Under Reagan and Shultz,* 19.
4. For a detailed treatment of the Cuban Missile Crisis case, see Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Longman, 1999).
5. Skoug, *The United States and Cuba Under Reagan and Shultz,* 27; Michael Wines and Ronald J. Ostrow, "Cuba Exults That CIA's Men in Havana Were Double Agents; In a Television Series, Alleged Spies-Turned-Heroes Tell How They Duped American Agency," *LA Times*, August 12, 1987.
6. For more information on the Multiple Hypotheses Generator™, go to http:// www.globalytica.com.
7. See Gary King, Robert O. Keohane, and Sidney Verba, *Designing Social Inquiry (*Princeton, NJ: Princeton University Press, 1994) for an extensive discussion about the principles of social science research; also see Richards J. Heuer Jr., *Psychology of Intelligence Analysis* (Reston, VA: Pherson Associates, 2007) for a discussion of cognitive issues affecting analysis.
8. Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, 2nd ed. (Washington, DC: CQ Press, 2015), 180.
9. Ibid., 185.
10. Skoug, *The United States and Cuba Under Reagan and Shultz,* 23.
11. Ibid., 56.
12. Susan B. Epstein and Mark P. Sullivan, *Cuba: Background and Issues Through 1994* (Washington, DC: Congressional Research Service), 2.
13. Skoug, *The United States and Cuba Under Reagan and Shultz,* 23.

Table 6.3 ▶ Case Snapshot: The Road to Tarin Kowt		
Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Key Assumptions Check	p. 209	Assessment of Cause and Effect
Devil's Advocacy	p. 260	Challenge Analysis
Strengths-Weaknesses-Opportunities-Threats	p. 308	Decision Support

6 The Road to Tarin Kowt
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

This case asks students to grapple not only with hard tactical and operational choices but also with implicit beliefs about economic and political development and their suitability for the region's culture. At the tactical and operational levels, the case presents several potential trade-offs: to build the road quickly might compromise the project's security; to proceed more deliberately could reduce its potential political impact. It also highlights some complex realities that demand a carefully considered approach. The people in the region are not only the villagers with whom relationships must be built to facilitate construction and generate support for central government; they are also the very insurgents with which the United States must contend, and it is unclear how many might be open to changing sides. The cultural code of Pashtunwali means that many locals will outwardly embrace and even aid US plans, but they will inwardly reject the incursion into their way of life; people who are assisting the project by day may very well be planting improvised explosive devices (IEDs) along the construction route by night.

At the strategic level, the case presents a contrast between local cultural norms and the transformational goals of the United States and—ostensibly—the Kabul government. One of the goals of this case is to teach students techniques that help them to uncover hidden assumptions underpinning policy options in order to troubleshoot policy plans and improve the odds of success. The techniques in this case help students to assess implicit beliefs about the operating environment, anticipated enemy response, and the potential impact on broader US goals for Afghanistan. Students should focus their efforts not on building the specific steps in a course of action but on identifying those issues that could not only undermine the immediate mission—completing the road—but also subvert the broader US goals in the region.

TECHNIQUE 1: KEY ASSUMPTIONS CHECK

The Key Assumptions Check is a systematic effort to make explicit and question the assumptions that guide an analyst's interpretation of evidence and reasoning about any particular problem. Assumptions are usually a necessary and unavoidable means of filling gaps in the incomplete, ambiguous, and sometimes deceptive information with which the analyst must work. They are driven by the analyst's education, training, and experience, including the cultural and organizational contexts in which the analyst lives and works. It can be difficult to identify assumptions, because many are sociocultural beliefs that are unconsciously or so firmly held that they are assumed to be truth and not subject to challenge. Nonetheless, identifying key assumptions and assessing the overall impact should they be invalid are critical parts of a robust analytic process.

Task 1.

Conduct a Key Assumptions Check of the following issue: The United States is leaning toward making a decision to complete the road from Kandahar to Tarin Kowt in time for the 18 September National Assembly elections as part of its broader goals to "spur economic development, promote central governance, and improve security."

Step 1: Gather a small group of individuals who are working on the issue along with a few "outsiders." The primary analytic unit already is working from an established mental model, so the "outsiders" are needed to bring other perspectives.

Step 2: Ideally, participants should be asked to bring a list of assumptions when they come to the meeting. If not, start the meeting with a silent brainstorming session. Ask each participant to write down several assumptions on 3 × 5 cards.

Step 3: Collect the cards and list the assumptions on a whiteboard for all to see. A simple template can be used, as in Table 6.4 in the book.

An initial list of brainstormed Key Assumptions for this case might include several higher-order assumptions such as the following:

- The local populace wants/needs the road.
- The Afghan government wants/needs the road.
- The US military wants/needs the road.
- The US military has the capacity to construct the road.
- The road will benefit the locals, the Afghan government, and US/NATO operations far more than it will benefit the Taliban.

Step 4: Elicit additional assumptions. Work from the prevailing analytic line back to the key arguments that support it. Use various devices to help prod participants' thinking. Ask the standard journalistic questions: Who? What? How? When? Where? and Why?

Phrases such as "will always," "will never," or "would have to be" suggest that an idea is not being challenged and perhaps should be. Phrases such as "based on" or "generally the case" usually suggest that a challengeable assumption is being made.

Asking these questions allows analysts to disaggregate and refine the initial brainstorming list. In this case, doing so reveals new, more nuanced assumptions and underlying assumptions. For example, an assumption about the Taliban's willingness to allow the road to be built underpins the key assumption that the road will benefit the locals, Afghan government, and US/NATO operations. These otherwise hidden assumptions bear consideration as well, and they should be captured in the Key Assumptions table.

Step 5: After identifying a full set of assumptions, critically examine each assumption. Ask:

- Why am I confident that this assumption is correct?
- In what circumstances might this assumption be untrue?
- Could it have been true in the past but no longer true today?
- How much confidence do I have that this assumption is valid?
- If the assumption turns out to be invalid, how much impact would this have on the analysis?

Step 6: Using Table 6.4, place each assumption in one of three categories:

1. Basically supported
2. Correct with some caveats
3. Unsupported or questionable—the "key uncertainties"

Table 6.7 shows an example classification of assumptions.

Table 6.7 ▶ Key Assumptions Check Example

Key Assumption	Commentary	Supported	With Caveat	Unsupported
The local population wants the road.	They may not want the asphalt road. Deep suspicions about outsiders may color local perceptions about the road's true purpose and likely impact on the region.		✓	
The local population needs the road.	The assumption is that they currently are limited by the absence of a road. They experience long travel times for commerce, goods, services, political participation, and security. Underlying assumption that a road would improve all of these. (See below for these assumptions.)		✓	
The local population will be able to use the road if it is built.	Will they feel safe using the road? Perhaps while the US military is there, but Soviet history suggests an ongoing security presence will be necessary.		✓	

Table 6.7 ▶ *(Continued)*

Key Assumption	Commentary	Supported	With Caveat	Unsupported
The code of Pashtunwali means that the locals will embrace and aid the project.	Hospitality and hostility go hand-in-hand in the code of Pashtunwali. The locals may embrace and even aid the project when interacting with the US Army but undermine it in the absence of US forces.		✓	
The Afghan leadership wants the United States to build the road.	The Afghan government lacks financing and capability but wants the road and wants the United States to build it.	✓		
The Afghan government can use the road to promote security, commerce, and governance.	This assumes that Afghan government has the necessary capacity to provide security, promote commerce, and improve governance. (See additional assumption about commerce below.)			✓
The US Army Engineers can build the road.	The US military has the range of capabilities but lacks paving capability.		✓	
A functioning road will benefit the Afghan government and US/NATO forces more than the Taliban.	The road will benefit anyone who can and does use it; this includes the Taliban, which may be interested in using the road for its own purposes.			✓
The Taliban will allow the road to be built.	Probably. It will see benefits from the road as well. (Stated another way, see below.)		✓	
The Taliban will not immediately destroy the road.	Maybe. The Taliban may try to assert control over the road, especially in this region, which is traditionally a Taliban stronghold. It may target US/NATO forces using the road with ambushes and IEDs.		✓	
There is no change in level of US/NATO commitment.	It is unclear at this point if the Karzai government will remain in power and if the United States will maintain its current level of commitment to Operation Enduring Freedom.		✓	
The road will increase commerce in the region.	The record of road usage during the Soviet occupation gives cause to question this assumption. Rather than improving commerce, roads provided the mujahidin with targets as they attacked Soviet supply lines.			✓
The road will improve security in the region.	The Soviet experience suggests the road could just as easily contribute to deterioration of security as increase security.			✓
The road will improve voter turnout in the parliamentary election.	It could increase participation, but this assumes that the voting stations will lie along the road and that the presence of outsiders (US military and others) will encourage participation rather than discourage it.			✓
Completion of the road in time for the election will produce greater voter support for candidates that favor the central Afghan government.	Unsupported. It cannot be assumed that a local culture that is inherently suspicious of outsiders and central government will be grateful that these outsiders have constructed a highway through its midst.			✓
The United States and its foreign contractors are the only ones who can build the road in time.	The key factor is the compressed schedule, which does not allow adequate time for the Army to hire and train a local construction crew.	✓		

Step 7: Refine the list, deleting those assumptions that do not hold up to scrutiny and adding new assumptions that emerge from the discussion.

This process reveals that it is important to amend assumptions to capture important nuances, such as by disaggregating the assumption that the local populace *wants* and *needs* the road. This process also reveals new assumptions that underpin initial assumptions. One example is the assumption that the road will improve commerce in the region and, in turn, that the Afghan government has the capacity to use it to promote commerce.

Step 8: Consider whether key uncertainties should be converted into collection requirements or research topics.

In this case, several key uncertainties stem from the assumption that the road will improve voter participation, security, commerce, and the central government's reach. Other key uncertainties are that a functioning road will benefit the Afghan government, locals, and US/NATO forces more than the Taliban and that the Taliban will continue to oppose US/NATO presence at its current, manageable level. Both of these warrant additional research into how much permanent security presence (US, NATO, or Afghan) will be required for the road's continued use.

Analytic Value Added: **What impact could unsupported assumptions have on the decision to build the road? How confident should military decision makers be that the benefits of building the road will outweigh the risks?** Much of the strategy is premised on assumptions that may be valid in the Western context but are questionable when applied to Pashtun culture. As a result, it cannot be assumed that the locals will be grateful for the road and will express that gratitude through participation in a democratic process. Neither can it be assumed that the locals—including the Taliban—intend to use the road in the ways envisioned by the United States.

Another key factor in this analysis is the behavior of the Taliban forces in the region. If the Taliban increases the magnitude of its campaign against the United States and cooperative locals, it could significantly affect the ability of the United States to build the road in a timely and secure manner and the road's impact on local opinion. The decision to pursue construction is based in part on the assumption that Taliban operations will remain at their current level and that the United States can suppress any change in that level.

TECHNIQUE 2: DEVIL'S ADVOCACY

Devil's Advocacy can be used to critique a proposed analytic judgment, plan, or decision. Devil's Advocacy is often used before a final decision is made, when a military commander or policy maker asks for an analysis of what could go wrong. The Devil's Advocate builds the strongest possible case against the proposed decision and its prospect for achieving its broader goals, often by examining critical assumptions and sources of uncertainty, among other issues.

Task 2.

Build the strongest possible case against the United States' pending decision to build the road from Kandahar to Tarin Kowt before the election.

Steps: Although there is no prescribed procedure for a Devil's Advocacy, begin with the strategic goals of the project, assumptions, and gaps. These can serve as a useful starting point from which to build the case against the road project. Next, build a logical argument that undermines each goal.

The best Devil's Advocate will identify the goals of US strategy and disassemble them, drawing from and augmenting the key assumptions and gaps identified in the previous exercise. Beginning with the strategic goals of the United States allows students to address the fundamental difficulties surrounding the broader security, economic, and political situation and then work downward to the more tactical issues facing the engineers as they embark on their mission. The argument might proceed as follows:

The USACE project will undermine the broader US goals of economic development, improved governance, and enhanced security in the region. The project is premised on the overarching assumption that the local population will welcome a highway constructed by outsiders and will express its gratitude by supporting the Karzai government in the September election and beyond. This assumption flies in the face of Pashtun culture, which is deeply distrustful of foreigners and central government. Through local eyes, the road is likely to be seen as a symbol of intrusion by invaders and would-be Kabul-based hegemons.

- **Commerce.** The project assumes that the road will spur licit local trade, but there is no indication that formal studies of its potential commercial impact have been done. Historical precedents provide

little basis for confidence that the road will have the intended commercial impact. Other Afghan roads have served as moneymakers for warlords, who extract tolls on truckers in return for allowing passage, and as transportation links for drug and arms traffickers.

- **Governance.** The project assumes that a compressed timeline will have a more salutary effect on local opinion than a slower and more patient approach. The case for an accelerated schedule is based on the belief that the locals will be impressed by the US engineering feat, will recognize its benefits for their daily lives, and will translate their gratitude into support for progressive forces in the September elections. A more likely outcome, however, is that locals will recoil at the rapidity with which outsiders intrude on their region. Most Pashtuns have little desire for links to Kabul and are unlikely to be grateful for construction of those links. By contrast, a slower timeline would allow the US Army to play a facilitating rather than a performing role, hiring and training a local construction force to build the road. This would have the best chance of investing the local population with ownership of the highway and avoiding the perception that the road is an externally imposed project.
- **Security.** Although the Army is equipped with many of the needed resources, the 864th Engineer Battalion cannot by itself provide sufficient security for the mission, given the threat along the road. Furthermore, the project assumes that once built, the road can function with little or no requirement for an ongoing US/NATO or Afghan government security presence. The Soviet experience was telling. Securing roads required massive deployments of forces, which proved impossible. In the absence of an ongoing Soviet security presence, mujahidin fighters took advantage of roads to ambush Soviet convoys with devastating effect. As a result, the roads did little to spur commerce, and Soviet forces never managed to extend control beyond major highways and population centers.

Analytic Value Added: Which issues could undermine the goals of the project, and why? Some students may be uncomfortable with a process that they perceive as second-guessing an order or task. It should be stressed to students that the goal of the exercise is to improve the chances of mission success by thinking as broadly and exhaustively as possible about potential impediments. When these potential impediments are exposed, decision makers can address them.

TECHNIQUE 3: STRENGTHS-WEAKNESSES-OPPORTUNITIES-THREATS

Strengths-Weaknesses-Opportunities-Threats (SWOT) can be used to evaluate a goal or objective by providing a framework for organizing and collecting data for strategic planning. SWOT is designed to illuminate areas for further exploration and more detailed planning, and therefore it is typically an early step in a robust policy process. SWOT analysis can also be an important part of troubleshooting a policy option and identifying specific actions that may improve the chances of success.

Task 3.

Conduct a SWOT analysis of the pending decision to spur economic development, promote central governance, and improve security in the region by building a road connecting Kandahar City to Tarin Kowt prior to the September election.

Step 1: Clearly define the objective.

Step 2: Fill in Table 6.5 in the book by listing the Strengths, Weaknesses, Opportunities, and Threats that are expected to facilitate or hinder achievement of the objective. Table 6.8 shows an example SWOT analysis.

Step 3: Identify possible strategies for achieving the objective by asking:

- How can we use each Strength?
- How can we improve each Weakness?
- How can we exploit each Opportunity?
- How can we mitigate each Threat?

Fill in Table 6.6 in the book with your strategies. Table 6.9 shows an example.

Analytic Value Added: What steps should the US Army take to prepare for road construction? The greatest benefits of the SWOT are that it encourages exhaustive and explicit thinking about each category and, in doing so, helps analysts to identify a number of practical steps that the United States should take to prepare for road construction.

Table 6.8 ▸ SWOT Example

US Strengths	US Weaknesses
▸ Knowledge, skills, equipment, logistics. ▸ Ability to secure immediate area around job site. ▸ Sufficient funding. ▸ Support of Afghan government.	▸ US soldiers and equipment are challenged by the extreme environment (heat/altitude/desert). ▸ United States faces cultural and linguistic barriers. ▸ The road is remote and far from the nearest base. ▸ Not enough security forces (infantry) are attached to the engineering battalion. ▸ No established network of local informers exists. ▸ Ephemeral presence in the region prevents establishment of relationships and fuels perception of US troops as outsiders.
Opportunities for the US	**Threats to the US**
▸ Engagement with a range of local villagers. ▸ Hiring and training of local construction force. ▸ Use of road for US logistics and lines of communication. ▸ Use of road to establish and maintain relations with a local network of informants. ▸ Research on potential commercial impact of road on local and regional economies.	▸ Easy target for Taliban harassment/ambush; Taliban could step up targeting. ▸ Taliban could exploit finished road to finance and support its own operations at the expense of the United States. ▸ Taliban could use the road for propaganda purposes to turn locals against the project. ▸ The US engineers will be blamed for any errors or accidents during construction. ▸ Supply line is threatened by the remote environment and by insurgents. ▸ Successful construction could saddle Afghan government with expensive upkeep.

Table 6.9 ▸ SWOT Second-Stage Analysis

Use Strengths	Improve Weaknesses
▸ The United States is positioned to build the base road quickly with US Army assets and USAID assistance.	▸ Construct logistic bases along road route and preposition needed supplies. ▸ Use local national interpreters and cultural advisors to identify tribal leaders. ▸ Establish small civil affairs units to work with local population. ▸ Request infantry and air assets in support of the mission. ▸ Rotate in new equipment or work at less hot times of the day.
Exploit Opportunities	**Mitigate Threats**
▸ Use early outreach to discuss and vet the route with local village elders. ▸ Use air superiority to deliver supplies. ▸ Use local construction forces when possible.	▸ Empower the village elders so that they see the benefits of the road and will be more inclined to accept any unforeseen problems that arise in construction. ▸ Use locals to deliver supplies and augment this with air supply. ▸ Use US Infantry units to flush out Taliban forces from surrounding mountains. ▸ Use of locals on construction teams could slow the process, but could redound to US advantage if it helps establish a workforce knowledgeable about road upkeep and capable of providing needed information about surrounding local and insurgent positions.

A robust SWOT analysis would delve deeper into these areas to develop plans to address each requirement:

- Conduct outreach with the local Afghan leaders to obtain buy-in for the road's route and locate adequate water supply and local logistics support and resupply.
- Identify interpreters and cultural advisors who have specific local knowledge.
- Coordinate with other US Army elements for security and resupply.

CONCLUSION

The United States ultimately committed to a compressed timeline to build the road. On 18 August 2005, Army engineers concluded road construction with a symbolic "meeting of the blades" at the midway point. The construction team, led by Task Force Pacemaker, included the US Army, the Afghan National Army, USAID, and international contractors, all of whom played important roles in meeting the deadline. The engineers spent over four months on overdrive to complete the road and credited success to careful and innovative planning and execution that drew on

> efficient use of equipment crew rotations, establishing and working from Forward Operating Bases, using material along the route, and relying on soldiers to adopt roles outside of their military occupational specialties . . .to streamline the process.[1]

The 864th Engineering Brigade arrived in Afghanistan organically equipped with heavy equipment, construction personnel, combat engineers trained to clear minefields and find hidden IEDs, and additional maintenance personnel and repair assets to assist with the vehicles and equipment. They also collaborated with other Army units in the area for infantry support. These units assisted with security missions on the road itself and patrols meant to flush out Taliban in the area. Logistical units ensured the flow of supplies, parts, and mail, in addition to providing sappers for route clearance operations and armored personnel carriers to safely transport the sappers. USAID contractors and subcontractors worked with the Army to pave the road. They provided supplementary heavy equipment, material testing services and laboratories, additional observation post support security for the forward operating bases, water wells, subsoil materials, and additional funding.[2], [3]

Instead of simply picking up where the 528th left off, working from south to north, the Pacemakers also began construction at the city of Tarin Kowt and worked south, establishing Forward Operating Base (FOB) Pacemaker at the midway point to support operations. At FOB Pacemaker, which was secured with a dirt berm perimeter and guard towers, the construction crews could safely store and maintain their equipment, eat, sleep, occasionally shower, and sometimes be able to call home.

The construction of the road to Tarin Kowt predates the United States' official adoption of the counterinsurgency doctrine (COIN). Although not a new concept, COIN defeats the goals of the enemy not primarily through kinetic operations against insurgents but by winning over the local population. As David Galula explained in his classic text on counterinsurgency warfare,

> if the insurgent manages to dissociate the population from the counterinsurgent, to control it physically, to get its active support, he will win the war because, in the final analysis, the exercise of political power depends on the tacit or explicit agreement of the population or, at worst, on its submissiveness.[4]

Task Force Pacemaker used local interpreters to ensure that the villages along the road were supported and friendly. The United States provided everything from security to standard infrastructure, with the hope that doing so would cause the insurgents to lose credibility among the local populace. Task Force Pacemaker built working relationships with the locals during the mission, but with the completion of the road the Army Engineers moved elsewhere, and the responsibility of maintaining partnerships with the communities fell on the local government officials and security forces.[5]

The tactical and operational success of Task Force Pacemaker is clear, but determining the extent to which this engineering feat advanced strategic US goals to "spur economic development, promote governance, and improve security" is difficult.[6] Between 2002 and 2007, the US government invested approximately $1.7 billion in road construction projects in Afghanistan. A 2008 study by the US Government Accountability Office (USGAO) found that

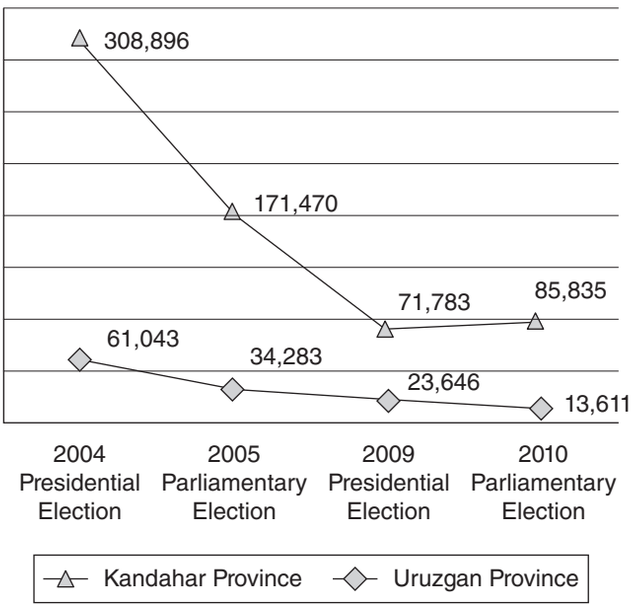
> the United States and other international donors have committed billions of dollars toward road reconstruction in Afghanistan to promote economic and social

development as well as security and stability. While some have noted that reconstructed roads contribute positively to economic and social conditions in Afghanistan, there is currently little evidence based on sound impact assessments that these projects have resulted in expected benefits. . . . [7]

The USGAO also stated that

[USAID] agency officials and others have reported some examples of projects' positive impact, such as increased commerce and decreased transportation costs. However, these results are based on a limited qualitative assessment or anecdotal information and therefore cannot be generalized.[8]

Figure 6.1 ▶ Voter Turnout by Election in Afghanistan, 2004–2010



Source: Compiled by the authors based on final election results released by the International Election Commission (IEC) of Afghanistan. The raw data are found at http://www.iec.org.af/.

USGAO found that between 2004 and 2007, the Department of Defense (DOD) spent nearly $15 million on Commanders' Emergency Response Program (CERP) projects in Kandahar and Uruzgan provinces, and USAID spent $25 million on the Kandahar City to Tarin Kowt road.[9] The US Army Corp of Engineers (USACE) reported to USGAO that general "impact indicators" it observed included increased traffic when a new road is built and more gas stations.[10] For the DOD, these developments underscored how the roads have improved governance by opening up lines of communication among districts, provinces, and the central government.[11] A senior Afghan security force leader working with Task Force Pacemaker, however, said he was afraid to travel to his home, only forty-five minutes away, noting that the Taliban "do not like the Tarin Kowt Road, and terrorize those who do"; he also predicted that "if the Americans pulled out, 'No one would travel down that road.' "[12] Upon completion of the road, the engineers no longer secured any areas along the route from Kandahar City to Tarin Kowt. The job of ensuring its safe accessibility fell to the Afghan security forces.[13]

Assessing the impact of the road on the election is further complicated by events surrounding election day itself and the inherent difficulty of isolating the road construction as an independent factor. One month after the Army completed the road, on 18 September 2005, Afghans headed to the polls in the first democratic parliamentary election since 1969. Voting took place amid Taliban threats of violence. The election results indicate a precipitous drop in voter turnout in both Kandahar and Uruzgan provinces between the 2004 presidential and 2005 parliamentary elections (see Figure 6.1). Countrywide voter turnout for the 2004 election was approximately 73 percent, while for the 2005 election it approached only 50 percent. The drop continued with the 2009 election, with turnout falling to 31 percent. For Uruzgan and Kandahar provinces, voter turnout fell from just over 40 percent to just over 20 percent combined. Isolating the precise impact of the road on voter turnout is impossible.[14] At best, it can be said that the road could have mitigated what otherwise would have been a more precipitous decline in voter turnout. At a minimum, the figures suggest the road did not have the catalytic effect on electoral participation that it was intended to have.

The road to Tarin Kowt has become a testimony to the gap between hope and reality in Afghanistan. When the US Army Engineers began to build the road in 2004, travelling the route along the dirt path linking the two cities took fifteen hours; immediately after the Army completed its work in 2005, the journey along the newly paved road took the engineers only three.[15] But within a few years, the road to Tarin Kowt had become one of the most dangerous roads in the world. Neither foreigners nor

Afghans could freely travel it for fear of attack by Taliban insurgents, and traffic was largely restricted to slow-moving biweekly convoys of 100 to 200 trucks.[16] The trucks were escorted by a local policeman who ran a force of about 300 uniformed police and another 1,700 militia.[17] In 2009, an Australian journalist chronicled a trip along the road, leaving Kandahar with an Afghan convoy at dawn and arriving in Tarin Kowt over twenty-four hours later. This journey along the modern road took nearly ten hours longer than travel along the centuries-old dirt path had taken.[18]

KEY TAKEAWAYS

- An effective Red Team approach can include a range of techniques and is an essential part of any process aimed at uncovering hidden weaknesses in a course of action. In this case, the approach helps to identify a misalignment of strategic, operational, and tactical goals.
- Even without an abundance of time or specialized knowledge, analysts can use these structured analytic techniques to identify the right questions to ask and to outline an approach that can mitigate weaknesses before they have deleterious effects on mission outcome.

NOTES

1. Laura M. Walker, "Task Force Pacemaker Constructing a Road to Democracy," *Army Engineer,* September–October 2005, 20.
2. Captain Claudia Crossland, US Army, interview with the authors, Virginia, July 6–7, 2010.
3. Elizabeth Wannstedt, "Meeting of the Blades," *Army Engineer,* September–October 2005, 30–31.
4. David Galula, *Counterinsurgency Warfare: Theory and Practice,* Westport, CT: Praeger Security International, 1964, 4.
5. Crossland, interview.
6. US Government Accountability Office, *Afghanistan Reconstruction Progress Made in Constructing Roads, but Assessments for Determining Impact and a Sustainable Maintenance Program Are Needed* (GAO-08–689), July 8, 2008, 5. Available at http://www.gao.gov/products/GAO-08–689.
7. Ibid., 38.
8. Ibid., 3.
9. Ibid., 47.
10. Ibid., 26.
11. Ibid.
12. Laura M. Walker, "Up Close . . . Task Force Pacemaker's Solders: Impressive Dedication and Professionalism," *Army Engineer*, September–October 2005, 26.
13. Crossland, interview.
14. The author compiled the raw voting data based on final election results released by the International Election Commission (IEC) of Afghanistan, which is the official election body. The raw data are found at http://www.iec.org.af. The mission of the IEC, which "is a constitutional body . . . and a professional Election management body" is to conduct "free and fair elections and referendums in an efficient and impartial way."
15. Walker, "Task Force Pacemaker Constructing a Road to Democracy," 19.
16. Bette Dam, "Danger on the Road to Uruzgan," *Radio Netherlands Worldwide (RNW) News*, July 10, 2009, http://hunaamsterdam.nl/english/article/danger-road-uruzgan.
17. Jeremy Kelly, "Long Road to Tarin Kowt," *The Australian*, April 28, 2008, http://www.theaustralian.com.au/news/world/longroad-to-tarin-kowt-story-e6frg6so-1225704435431.
18. Ibid.

Table 7.1 ▶ Case Snapshot: Who Murdered Jonathan Luna?

Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Chronologies and Timelines	p. 56	Decomposition and Visualization
Simple Hypotheses	p. 171	Hypothesis Generation and Testing
Multiple Hypotheses Generator™	p. 173	Hypothesis Generation and Testing
Analysis of Competing Hypotheses	p. 181	Hypothesis Generation and Testing

7 Who Murdered Jonathan Luna?
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

The Luna case has never been solved. It is not a puzzle for which there is a correct and final answer that points to a killer, whether it is Luna himself or someone else. When confronting a case in which so much significant information is unknown, the analyst should focus first on devising and executing a solid analytic process that frames the problem and brings order to the jumble of data points, assumptions, and gaps that form the case. In short, the focus is on defining an analytic process now that will increase the chances that the analyst will identify and incorporate emerging information to help solve the puzzle in the future.

The controversy surrounding this case as well as the detailed information that is already publicly available makes it a particularly good tool for teaching how analytic techniques such as Timelines, Chronologies, Hypothesis Generation, and Analysis of Competing Hypotheses can help analysts systematically sort, array, and analyze a data set in a way that brings a complex group of events into better, if not complete, focus. It also drives home how geospatial visualization tools such as mapping software can illuminate analytic points that otherwise may be overlooked, such as anomalies in distance, timing, and location information. Lastly, as with all cases in which human, electronic, and press reporting are used, the case highlights the importance of both sourcing and confidence levels in analysis, particularly when dealing with eyewitnesses, secondhand reporting, and after-the-fact recollections.

TECHNIQUE 1: CHRONOLOGIES AND TIMELINES

Chronologies and Timelines are simple but useful tools that help order events sequentially; display the information graphically; and identify possible gaps, anomalies, and correlations. In addition, these techniques pull the analyst out of the evidentiary weeds to view a data set from a more strategic vantage point. Chronologies and Timelines can be paired with mapping software to create geospatial products that display multiple layers of information such as time, location, terrain, weather, and other travel conditions.

The details of this case make an annotated Timeline and Map particularly useful in identifying key pieces of evidence, confidence levels in the reporting, and gaps in the information.

Task 1.

Create a Timeline of Luna's last hours.

Step 1: Identify the relevant information from the case narrative with the date and order in which it occurred. Consider how best to array the data along the Timeline. Can any of the information be categorized?

There are many ways to present the data in this case in a timeline. A full timeline of the case will reflect a period from Luna's youth in New York through his death and into the present day. It will include all references in the case to Luna's activities prior to his death and new information uncovered in the investigation. This new information should be reflected on the timeline at the time it allegedly occurred. A more sophisticated timeline would also include a separate line for when the information was reported. Doing so not only helps an analyst see events as they unfolded but also understand when information became available. This allows analysts to look for any anomalies in the pattern of the reporting that might be associated with a deception hypothesis.

The timeline in Figure 7.1 is excerpted from a longer timeline of the case and illustrates how relevant information can be displayed along a two-sided timeline in order to reflect evidence and analysis, including assumptions and gaps. It also shows how color coding can be used to reflect categories of activities. In this timeline, the evidence is broken into three categories: Luna's known movements, the car's movements, and his bank card activities.

Step 2: Review the Timeline by asking the following questions:

- Are there any missing pieces of data?

There is a lack of information about Luna's activities between 1730 and his return to the office after 2300 that night. This gap raises a number of important questions. For instance, what time did he arrive at home? Did he go directly home? When exactly did he leave for the office later that night? Where was he when he called opposing counsel?

- Do any of the events appear to occur too rapidly or slowly to have reasonably occurred in the order or timing suggested by the data?

At the time of the investigation, authorities said that they could not account for a two-hour period beginning at 0057, when Luna's ATM card was used at a rest stop in Delaware, and ending at 0247, when his car passed through the Delaware River Bridge toll plaza on Interstate 276.[1] The earliest, judging by driving times, that he could have entered the Pennsylvania Turnpike would have been 0145, but the E-ZPass record indicates that the car did not enter the Turnpike until 0247. In addition, the timing of the King of Prussia and Elverson Roy Rogers stops seems too close. It seems unlikely that Luna would have been able to travel that far in such a short period of time.

- Could any events outside the timeline have influenced the activities?

Possibly. Given the unexplained gaps outlined above, events could have occurred during these gaps that have direct bearing on the timeline.

- Are there any underlying assumptions about the evidence that should be taken into consideration?

The sources of information include eyewitnesses and confidential sources. For the purposes of the timeline, we have assumed that these sources as reported are accurate, and we have included them on the timeline. When there are questions about the reliability of reporting, or there are anomalies, these can be listed on the timeline as an analytic comment. In this timeline, analytic comments are reflected in italics above the timeline.

Task 2.

Create an annotated Map of events based on your Timeline.

Step 1: Use publicly available software of your choosing to create a Map of the area.

Step 2: Overlay the route.

Step 3: Annotate the Map with appropriate times and locations presented in the case (see Map 7.2).

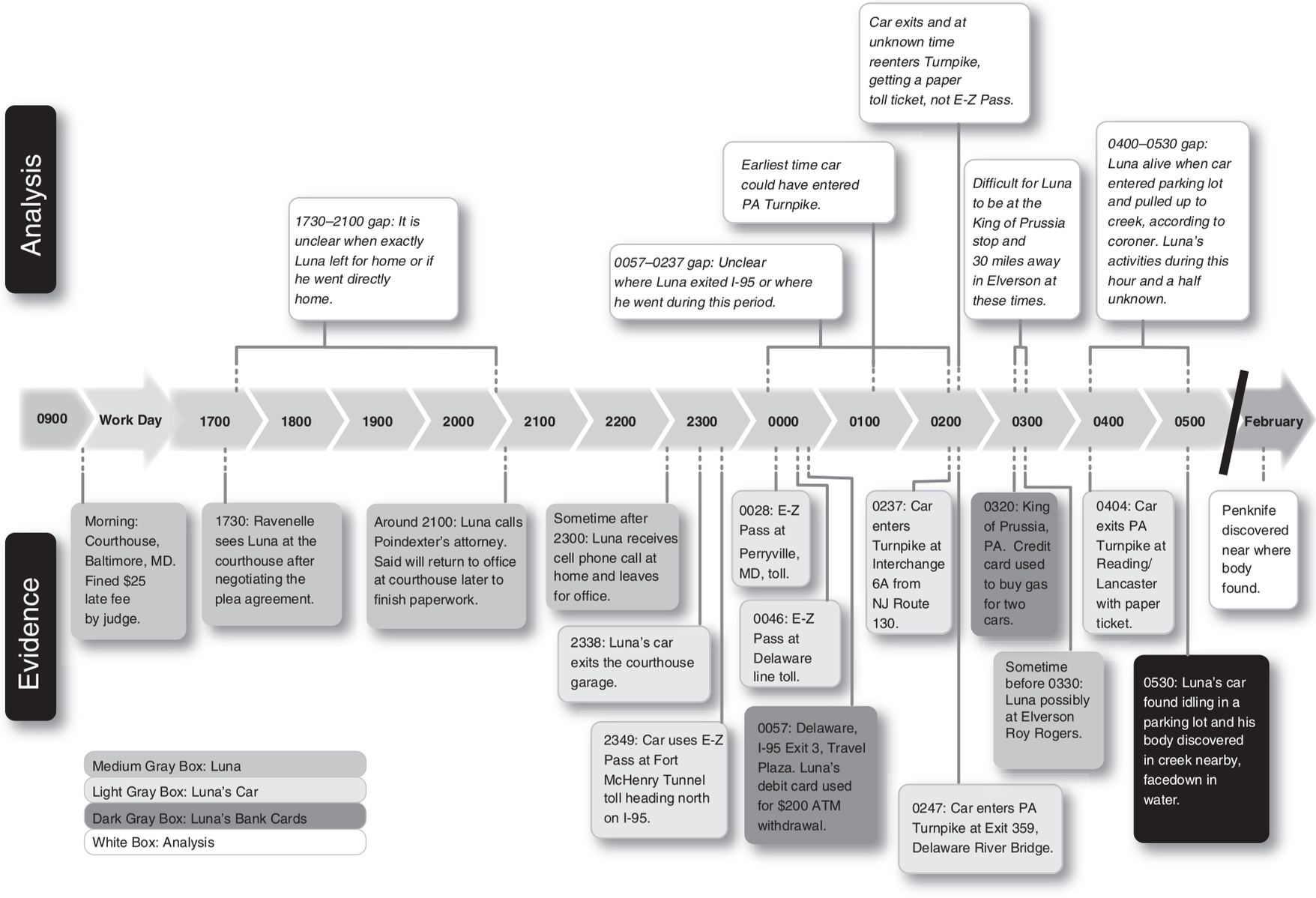
For those seeking to employ a more sophisticated geospatial presentation, geographic coordinates are included with key data points in Table 7.2.

Analytic Value Added: **What does the sequence of events tell you?** From the time Luna left his home until the time his body was found in Pennsylvania on the morning of 4 December 2010, we have only information about his car and bank card. From Map 7.2, it appears that Luna took a roundabout route from his Baltimore office to Lancaster, Pennsylvania. He drove northeastward on I-95 from Baltimore to Delaware and then toward the Philadelphia area, but then veered westward on the Pennsylvania Turnpike.

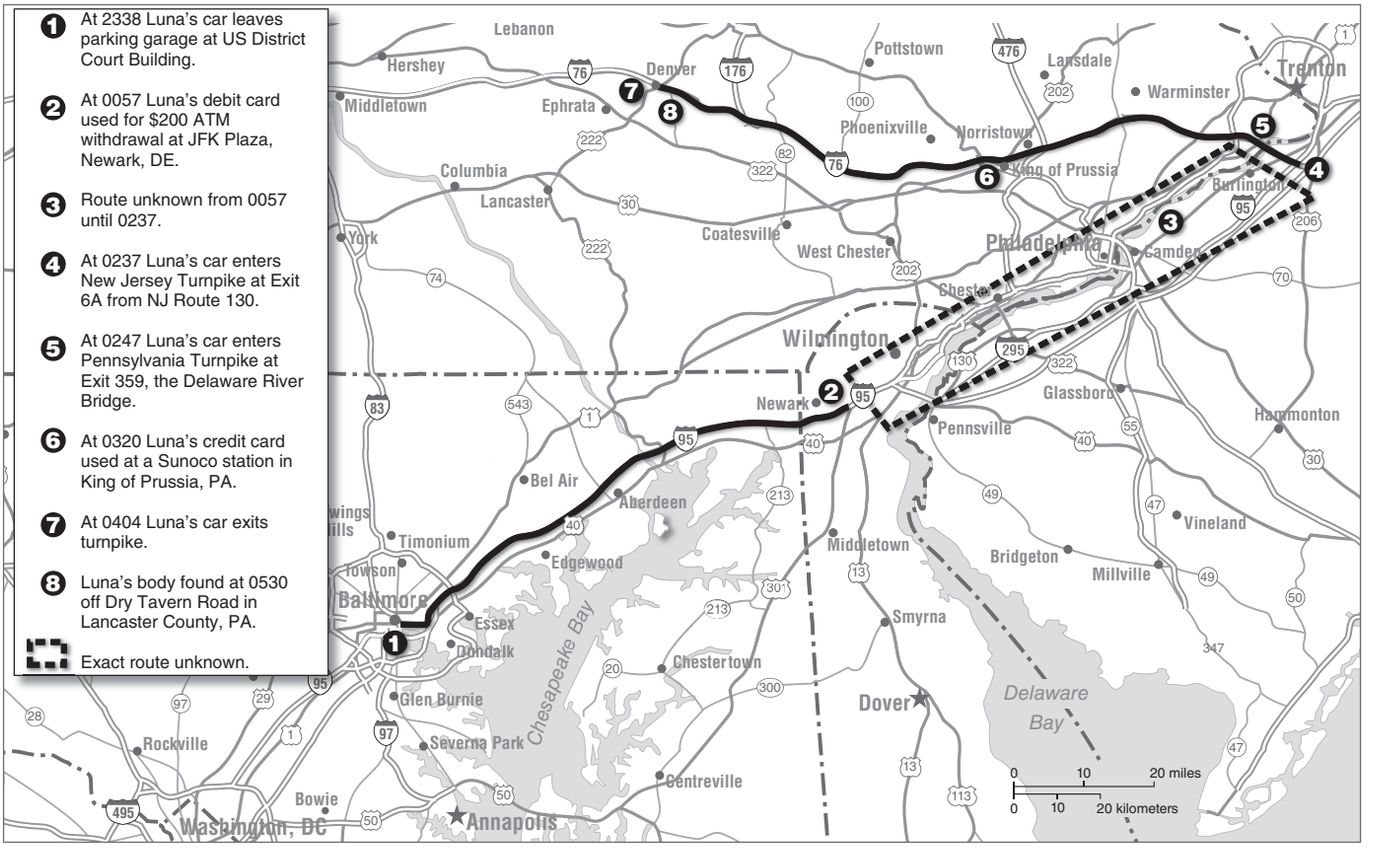
Are there any gaps in the information that should be addressed? There are gaps between 1730 and 2100, 0057 and 0237, and 0404 and 0530. There are conflicting reports about his whereabouts between 0300 and 0400. The 0057 to 0237 period is most perplexing, because is unclear what route he took from the JFK rest stop to New Jersey Turnpike interchange 6A from New Jersey Route 130. Did he make any stops during that period?

What additional information should you seek? There is a lack of information that would determine whether he was alone or with someone, whether he was the driver for the entire trip, or whether he was the user of the debit card. A second driver, for example, could have used a paper ticket, not realizing that the car was equipped with E-ZPass.

Figure 7.1 ▶ Timeline Excerpt: Jonathan Luna's Last Hours



Map 7.2 ▶ Jonathan Luna's Movements during His Final Hours



Additional information should be sought about his route and activities from 0057 until 0237.

How confident are you in the sources of information? Much of the reporting comes from unnamed law enforcement sources, eyewitness reports, or character witnesses. As a result, the analysis should reflect the reliability of these sources, particularly when there are conflicting or anomalous aspects to the reporting. Also, for electronic evidence, such as building records, E-ZPass, and bank records, confidence levels and underlying assumptions should be noted; while the reporting probably reflects accurate time stamps, it is unknown if Luna himself was the user of the car and debit cards at all times.

TECHNIQUE 2: MULTIPLE HYPOTHESIS GENERATION: SIMPLE HYPOTHESES

Multiple Hypothesis Generation is part of any rigorous analytic process because it helps the analyst avoid common pitfalls such as coming to premature closure or being overly influenced by first impressions. Instead, it helps the analyst think broadly and creatively about a range of possibilities. The goal is to develop an exhaustive list of hypotheses that can be scrutinized and tested over time against both existing evidence and new data that may become available in the future.

This case is well suited to Simple Hypotheses, which employs a group process that can be used to think creatively about a range of possible explanations that go beyond those raised by authorities in the case. Using a group helps to generate a large list of possible hypotheses; group the lists; and refine the groupings to arrive at a set of plausible, clearly stated hypotheses for further investigation.

Task 3.

Use Simple Hypotheses to create a list of alternative hypotheses that explain Jonathan Luna's death.

Step 1: Ask each member of the group to write down on separate 3 × 5 cards or sticky notes up to three plausible

Table 7.2 ▶ Jonathan Luna's Route with Geographic Coordinates

Date	Time	Location	Activity	Geo-coordinates
Wednesday 3 December	2338	Court House, Baltimore, MD	Luna's car leaves parking garage at US District Court Building.	39°17'13.21"N 76°37'2.43"W
	2349	Baltimore, MD	Luna's car passes Fort McHenry Tunnel toll plaza, northbound on I-95.	39°15'39.12"N 76°34'38.87"W
Thursday 4 December	0028	Perryville, MD	Luna's car passes through Perryville toll plaza, northbound.	39°35'15.68"N 76° 4'24.15"W
	0046	Delaware Line toll plaza	Luna's car passes through toll plaza, northbound.	39°38'42.39"N 75°45'52.56"W
	0057	I-95 Exit 3, Newark, DE	Luna's debit card was used for a $200 ATM withdrawal from Exxon at Travel Plaza.	39°39'45.30"N 75°41'25.71"W
	0237	New Jersey Turnpike	Luna's car enters Turnpike at interchange 6A from NJ Route 130.	40° 6'5.78"N 74°47'21.25"W
	0247	Delaware River Bridge, PA	Luna's car enters Pennsylvania Turnpike at interchange 359, the Delaware River Bridge.	40° 7'18.18"N 74°50'46.90"W
	0320	King of Prussia, PA	Luna's debit card was used at a Sunoco Station to buy gas and possibly for another ATM withdrawal.	40° 5'22.03"N 75°22'15.61"W
	0330	PA Turnpike, Elverson, PA	A Roy Rogers restaurant manager at a rest stop says she saw Luna. FBI investigators doubt this.	40° 8'58.46"N 75°49'59.85"W
	0404	PA Turnpike, the Reading/ Lancaster interchange	Luna's car exited PA Turnpike at exit 286. Paper ticket (with blood spot) was turned in to toll collector even though Luna's car has E-ZPass.	40°12'58.97"N 76° 4'29.27"W
	After 0530	Denver, PA	Sensening & Weaver employee finds Luna's car on company property, hood down in a creek.	40°12'37.45"N 76° 3'30.58"W

alternative hypotheses or explanations. Think broadly and creatively but strive to incorporate the elements of a good hypothesis:

- It is written as a definite statement.
- It is based on observations and knowledge.
- It is testable and falsifiable.
- It contains a dependent and an independent variable.

Step 2: Collect the cards and display the results. Consolidate the hypotheses to avoid duplication. A consolidated set of hypotheses might look like Table 7.3.

Step 3: Aggregate the hypotheses into affinity groups and label each group.

Consider multiple ways to display the affinity groups. In this case, the hypotheses may be grouped by perpetrator of the crime, which includes Luna himself (the suicide

Table 7.3 ▶ Luna Simple Hypothesis Generation: Example of Consolidated Hypotheses

Luna was murdered by those he was negotiating a plea bargain for; they did not like the deal.
Luna committed suicide.
Luna was killed by someone associated with another case he had worked.
Luna was murdered by a female or male lover in an established relationship.
Luna was murdered by the established lover's spouse.
Luna was abducted and murdered by creditors for his failure to pay off bad debts.
Luna had a liaison with someone he had just met on an Internet sex site, and the affair went bad, resulting in his stabbing. He fell into a creek and died.
His wife had him killed because she found out he was cheating.
Luna's attorney colleagues were jealous of him and had him killed/ killed him.
Luna was being blackmailed and the operation went bad and they killed him.

hypothesis), a lover, a hit man, Luna's colleagues, etc. Alternatively, grouping by Why (debt, work-related issues, jealousy/envy, and random violence), for example, can help considerably with achieving mutual exclusivity and can help consolidate the Who list later.

Step 4: Use problem restatement and consideration of the opposite to develop new ideas.

Problem Restatement: Why did Jonathan Luna take such a circuitous and late-night trip toward Philadelphia?

Opposite: Luna was not suicidal; he was a victim of someone else's rage. This could include a random act of violence or a murder by a lover, colleague, criminal he had previously prosecuted, or creditor.

This process illuminates the possibility of a random act of violence. Luna had allegedly traveled to Philadelphia numerous times. His circuitous route that night took him first directly toward Philadelphia. Only after the anomalous two-hour period from the 0057 ATM withdrawal to 0247 did his car take a turn westward. Could he have been headed to Philadelphia and fallen victim to a random act of violence on his trip? Luna's key witness in the case he had been prosecuting that day, who had reversed himself on the stand, had been in custody in Philadelphia. Could Luna have been returning to Philadelphia for work-related purposes?

Step 5: Update the list of alternative hypotheses.

Problem restatement augments the list of hypotheses by including the possibility of a random act of violence.

Step 6: Clarify each hypothesis by asking, Who? What? How? When? Where? and Why?

Make a list of each of the categories above. Step back and consider how each list could be augmented. The Who list includes colleagues, stranger, lover, creditors, criminal he had prosecuted in the past. Refine this list to make the categories more mutually exclusive. This helps clarify the hypotheses. For example, creditors, criminals, and colleagues could all have employed a hit man.

Step 7: Select the most promising hypotheses for further exploration.

Luna was murdered by those he was negotiating a plea bargain for, his creditors, or his lover; Luna committed suicide; Luna was killed in a random act of violence.

TECHNIQUE 3: MULTIPLE HYPOTHESIS GENERATION: MULTIPLE HYPOTHESES GENERATOR™

The Multiple Hypotheses Generator™ is a useful tool for broadening the spectrum of plausible hypotheses. It is particularly helpful when there is a reigning lead hypothesis—in this case, the hypothesis that Luna was alone the night he died and therefore must have committed suicide.

The most important aspect of the tool is the discussion it generates among analysts about the range of plausible hypotheses, especially about the credibility score for each permutation. It is important to remember that the credibility score is meant to illuminate new, credible hypotheses for further examination. And while the process does encourage analysts to focus on the hypotheses with higher credibility scores, hypotheses with low credibility scores should not be entirely discarded because new evidence may emerge that changes their status.

Task 4.

Use the Multiple Hypotheses Generator™ to create and assess alternative hypotheses that explain Jonathan Luna's death. Contact Globalytica, LLC at THINKSuite@globalytica.com or go to http://www.globalytica.com to obtain access to the Multiple Hypotheses Generator™ software if it is not available on your system.

Step 1: Identify the lead hypothesis and its component parts using Who? What? How? When? Where? and Why?

Jonathan Luna committed suicide as a result of "personal problems," including debt and a possible investigation of personal wrongdoing.

Steps 2 & 3: Identify plausible alternatives for each key component and strive to keep them mutually exclusive. Discard any "given" factors.

Discard How (drowning), Where (Pennsylvania), What (killed), When (4 December 2003), which will be the same for all hypotheses. Brainstorm possible alternatives for each of the remaining components, which in this case are Who and Why. Consolidate the lists into alternatives that are as mutually exclusive as possible. For example, *adversary* is used in the example in Table 7.4 to reflect Luna's enemies or someone who is hired by or is associated with those who would want to kill Luna. A random attacker could reflect a robbery or hate crime.

Table 7.4 ▶ Luna Multiple Hypotheses Generator™: Examples of Brainstormed Alternatives

Lead Hypothesis: Jonathan Luna committed suicide as a result of personal problems he was facing.

Components	Who?	Why?
Lead Hypothesis	Suicide (Luna)	Debt
Brainstormed Alternatives	Adversary/Hit Man Lover Random Attacker	Work-Related Problem Jealousy/Envy Accident

Steps 4, 5, & 6: Generate a list of possible permutations, discard any permutations that simply make no sense, and evaluate the credibility of the remaining hypotheses on a scale of 1 to 5, where 1 is low credibility and 5 is high credibility.

Table 7.5 shows an example response.

Step 7: Re-sort the remaining hypotheses, listing them from most to least credible.

Table 7.6 shows an example.

Step 8: Restate the permutations as hypotheses.

The permutations in Table 7.6 are stated as hypotheses.

Step 9: Select from the top of the list those alternative hypotheses most deserving of attention and note why these hypotheses are most interesting.

For this case, this includes hypotheses with a credibility score of 3 or higher (see Table 7.7). While the credibility score is subjective in nature, it should reflect reasoning that can be used to weed out nonsensical or highly unlikely hypotheses. The unused hypotheses should not be discarded. They should be reserved, and the list should be reconsidered as new information becomes available.

Analytic Value Added: **Which hypotheses should be explored further?** For this case, the lead hypothesis, that Luna committed suicide, should certainly be further explored, as should the new random act of violence hypothesis.

What motives should be considered, and why? A full set of motives, including jealousy, envy, his debt, his work, or accident should also be explored.

Which hypotheses from the original list were set aside, and why? It is up to the analyst to decide how many and which hypotheses should be considered for further exploration. A general rule of thumb is that more than

Table 7.5 ▶ Luna Multiple Hypotheses Generator™: Example of Permutations and Credibility Scoring

Who?	Why?	Permutations	Credibility Score
Suicide	Debt	Luna committed suicide because he was in debt.	2
	Work-related	Luna committed suicide because he was having problems with work.	5
	Jealousy/envy	Luna committed suicide because of problems with a lover.	1
	Accident	Luna committed suicide accidentally.	5
Adversary/ Hit Man	Debt	Adversary killed Luna because of his indebtedness.	4
	Work-related	Adversary killed Luna because of his performance on a case at work.	5
	Jealousy/envy	Adversary killed Luna out of envy.	1
	Accident	Adversary killed Luna accidentally.	1
Lover	Debt	A lover killed Luna because of Luna's debt.	1
	Work-related	A lover killed Luna because of his performance on a case at work.	1
	Jealousy/envy	A lover killed Luna out of jealousy.	3
	Accident	A lover accidentally killed Luna.	2
Random Attacker	Debt	A random attacker killed Luna because of his indebtedness.	1
	Work-related	A random attacker killed Luna because of his performance on a case at work.	1
	Jealousy/envy	A random attacker killed Luna out of envy.	3
	Accident	A random attacker killed Luna accidentally.	2

Table 7.6 ▶ Luna Multiple Hypotheses Generator™: Example of Sorted and Scored Hypotheses

Permutation	Credibility
Luna committed suicide because he was having problems at work.	5
Luna committed suicide accidentally.	5
Adversary killed Luna because of his performance on a case at work.	5
Adversary killed Luna because of his indebtedness.	4
A lover killed Luna out of jealousy.	3
A random attacker killed Luna out of envy.	3
Luna committed suicide because he was in debt.	2
A lover accidentally killed Luna.	2
A random attacker killed Luna accidentally.	2
Luna committed suicide because of problems with a lover.	1
Adversary killed Luna out of envy.	1
Adversary killed Luna accidentally.	1
A lover killed Luna because of Luna's debt.	1
A lover killed Luna because of his performance on a case at work.	1
A random attacker killed Luna because of his indebtedness.	1
A random attacker killed Luna because of his performance on a case at work.	1

Table 7.7 ▶ Luna Multiple Hypotheses Generator™: Example of Hypotheses for Further Exploration

Hypotheses for Further Exploration	Reasoning
Luna committed suicide because he was having problems at work.	Suicide—whether intentional or unintentional—is authorities' lead hypothesis; authorities have heretofore undisclosed reasons to believe Luna was alone the night of his death.
Luna committed suicide accidentally.	The main motivation for such an accidental suicide has been reported as being an effort to garner sympathy and/or stave off taking a polygraph in connection with an ongoing investigation.
Adversary killed Luna because of his performance on a case at work.	His profession makes him a possible target of many individuals. Whether the death was a "hit" or an attack by a known acquaintance, the work-related adversary hypothesis should be explored further.
Adversary killed Luna because of his indebtedness.	Luna had credit card debt. Were there any other debts that could have prompted an adversary to intentionally or unintentionally take his life?
A lover killed Luna out of jealousy.	The so called "personal nature" of the attack, including wounds to the genitals, could point to a lover's involvement.
A random attacker killed Luna out of envy.	Given stops along the roundabout route and gaps in information concerning the route itself after the 0057 withdrawal, must consider a random attacker.

five hypotheses becomes cumbersome and should signal possible problems with mutual exclusivity. In such cases, analysts should be encouraged to aggregate hypotheses or review the basis for the credibility scoring. Also, analysts often will include hypotheses for which there is no evidence in the original list. In this case, students may raise the possibility that Luna was murdered by his spouse. This kind of creative thinking should not be discouraged in the initial brainstorming phase, but hypotheses that are not based on observations or knowledge should not

constitute the lead hypotheses for further exploration. Analysts should, however, explicitly discuss why certain hypotheses do not make the final list and how that could change in the future should new information come to light.

TECHNIQUE 4: ANALYSIS OF COMPETING HYPOTHESES

Analysts face a perennial challenge of working with incomplete, ambiguous, anomalous, and sometimes deceptive data. In addition, strict time constraints on analysis and the need to "make a call" often conspire with a number of natural human cognitive tendencies to zero in on a single hypothesis too early in the analytic process. The result is often inaccurate or incomplete judgments. Analysis of Competing Hypotheses (ACH) improves the analyst's chances of overcoming these challenges by requiring the analyst to identify and refute possible hypotheses using the full range of data, assumptions, and gaps that are pertinent to the problem at hand.

Task 5.

Use the top hypotheses compiled with the Multiple Hypotheses Generator™ to conduct an Analysis of Competing Hypotheses of the Luna case. Contact Globalytica, LLC at THINKSuite@globalytica.com or go to http://www.globalytica.com to obtain access to the basic software, or the collaborative version called Te@mACH®, if it is not available on your system.

Step 1: List the hypotheses to be considered, striving for mutual exclusivity.

The Multiple Hypotheses Generator™ and Simple Hypotheses techniques help to ensure mutual exclusivity and an exhaustive set of hypotheses, which greatly aids the utility of ACH.

ACH matrices can include as many hypotheses as the analyst requires. However, more than five hypotheses usually become cumbersome and reflect a problem with mutual exclusivity. In this case, there is some overlap with the suicide, but the motivations (accidental versus intentional suicide) are sufficiently exclusive of one another to retain both hypotheses in the matrix. As a result, a notional list might include: Luna committed suicide because of problems at work; Luna accidentally committed suicide; an adversary killed Luna because of his performance on a case at work; a lover killed Luna out of jealousy; a random attacker killed Luna out of envy.

Step 2: Make a list of all relevant information, including significant evidence, arguments, gaps, and assumptions.

Figure 7.2 shows an example of list of information.

Step 3: Assess the relevant information against each hypothesis by asking, "Is this information highly inconsistent, inconsistent, neutral, not applicable, consistent, or highly consistent vis-à-vis the hypothesis?" (The Te@mACH® software does not include the "neutral" category.)

Analysts using the basic ACH software will have the option of choosing highly consistent (CC), consistent (C), inconsistent (I), highly inconsistent (II), not applicable (NA), or neutral (N). When using basic ACH or My Matrix with the Te@mACH® tool, it is important that analysts code the evidence line by line, in other words horizontally across the matrix, not hypothesis by hypothesis, or vertically down the matrix. Doing so helps the analyst consider each piece of evidence fully against each hypothesis before moving on to the next piece of evidence. This process keeps the analyst focused on the evidence rather than on proving a pet hypothesis. The "Survey" option in Te@mACH® generates the cells randomly, avoiding this problem.

When entering and coding the data, the credibility score of all evidence is set at a default of medium. Analysts can also include a credibility score of low or high. Doing so when using the basic ACH tool will allow the ACH software to calculate a weighted inconsistency score that reflects the analysts' judgment about credibility of the data. For this case, the credibility of evidence is particularly important. Direct, expert evidence from coroner Dr. Barry Walp, for example, could be coded as highly credible, while indirect evidence from anonymous law enforcement sources may simply remain medium. DiBagio's contradictory reporting could be coded as low. Any credibility issues incorporated into the matrix should be included in the final, written analysis, because they are assumptions embedded in the analysis. With Te@mACH®, you can check a special "Key Assumptions" box to record and explain any key assumptions relating to a particular item of relevant information. Figure 7.3 shows coding matrices for two ACH software packages.

Step 4: Rate the credibility of each item of relevant information.

Step 5: Refine the matrix by reconsidering the hypotheses. Does it make sense to combine two hypotheses, add a new hypothesis, or disaggregate an existing one?

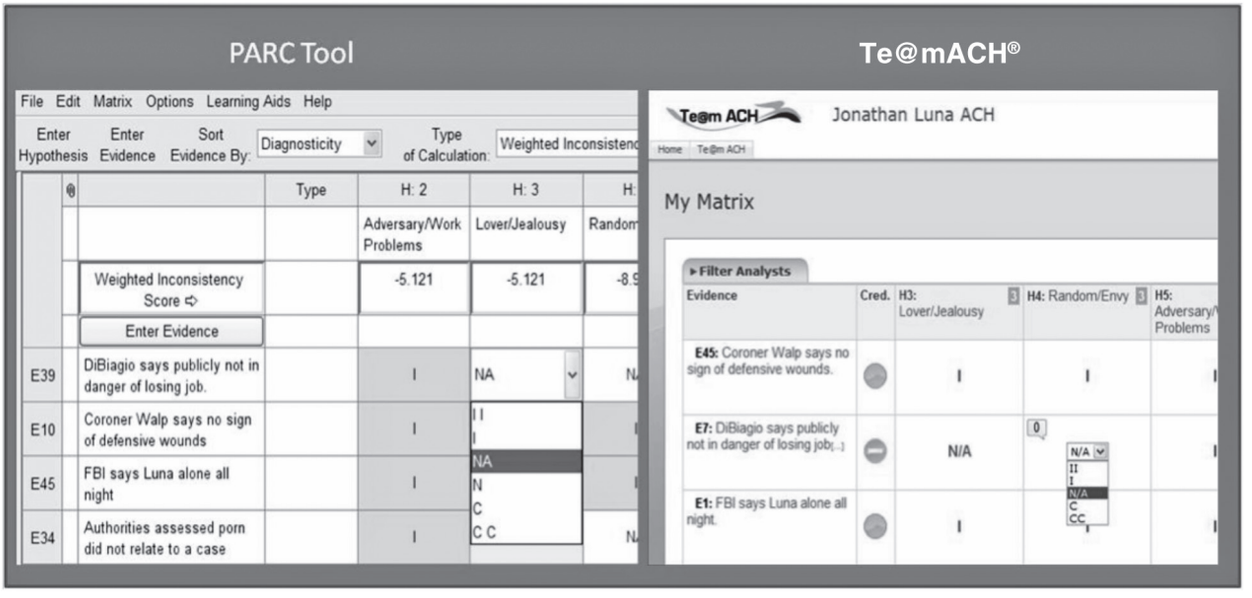
Figure 7.2 ▶ Jonathan Luna Case: Basic List of Evidence for ACH

- FBI says Luna alone all night.
- Blood of second person in car.
- Blood on paper toll ticket.
- Killed by own penknife.
- Many prick marks on body.
- Left phone and eyeglasses in office.
- DiBiagio says publicly not in danger of losing job.
- Luna felt job in peril.
- Gas station attendee says saw Luna late at night about once a month over six-month period.
- Colleagues say Luna took trips to Philadelphia for case.
- Luna sought sex with women on Internet sites.
- Authorities assessed porn did not relate to the case.
- Pornographic files on computer.
- Filed, then withdrew, loan application.
- Hid some debt from wife.
- $25K in debt on at least 16 credit cards.
- Walp classifies as homicide.
- Body discovered off Dry Tavern Road.
- Plea agreement because of problem with FBI witness.
- Coroner (Kirchner) classifies as homicide.
- Pool of blood in back seat.
- Traumatic neck wound.
- Allegations that FBI mishandled informant.
- Source says Luna came into $10K just as $36K in evidence went missing.
- DiBiagio privately admitted to coworkers that he had lied about Luna's job being in jeopardy.
- Internal FBI inquiry into FBI's handling of allegations of agent's affair with Luna.
- Roy Rogers at 0330, timing odd.
- Luna appeared calm at Sunoco.
- Investigators say 99% sure a second car not with him.
- Took a paper ticket rather than E-ZPass.
- Gap between 0057 and 0247; don't know route.
- Bought gas for two cars.
- ATM withdrawal of $200.
- Headed northbound on I-95.
- Only at office a few minutes.
- Planned to fax plea agreements to defense by morning.
- Currently negotiated plea agreement that resulted in lesser charges for defendants.
- Currently prosecuting drug conspiracy case.
- Previously prosecuted violent offenders.
- He and his wife "perfect couple."
- As of 1999 excited, idealistic.
- Law school class president.
- Brought up in rough neighborhood.
- Died of drowning.
- Coroner Walp says no sign of defensive wounds.
- Luna showed signs of defensive wounds.
- Signs of restraint.
- Injuries to genitals.
- 36 stab wounds (coroner).
- Fully clothed, wallet, money, work identification.
- Luna's body facedown in creek.
- Money and cell phone equipment scattered throughout car.
- Blood on driver's door and left front fender.
- Luna's car found nose down in creek, still idling.

If the hypotheses are not mutually exclusive, this fact will become apparent at this stage in the process if it has not already become so during the coding process. Analysts should consider disaggregating hypotheses whenever they find themselves "clarifying" the hypothesis as they code. Such is the case if one only considers a basic suicide hypothesis. As evidence is coded, it will become apparent that a separate, accidental/staged suicide hypothesis is necessary. The trigger, or indicator, that this is necessary occurs during the coding process. If a piece of evidence that is inconsistent with intentional suicide is often clarified by "But it could be consistent if he was trying to stage the attack and it went wrong," then another hypothesis is needed.

Step 6: Draw tentative conclusions about the relative likelihood of each hypothesis. An inconsistency score will be calculated by the software; the hypothesis with the lowest inconsistency score is tentatively the most likely hypothesis. The one with the most inconsistencies is the least likely. The hypotheses with the lowest scores appear on the left of the matrix, and those with the highest inconsistency scores appear on the right.

Figure 7.3 ▶ Luna PARC ACH and Te@mACH® Coding Differences in Matrix View



It is important to address the likelihood of every hypothesis, not simply the most and least likely. Based upon the above hypotheses and relevant information, some tentative conclusions about the relative likelihood of each hypothesis would include the following observations. It appears that an intentional, work-related suicide is by far the least likely hypothesis because it has the most inconsistent evidence. Another less likely hypothesis is the accidental suicide hypothesis—that Luna killed himself while attempting to stage an attack on himself. For example, it makes little sense that he would inflict injury to his own genitals or that blood of a second person would be present. Likewise, a random attack is nearly as unlikely as accidental suicide; a case can be made that a random attacker would not use the victim's own penknife. And finally, although a jealous lover hypothesis is the least inconsistent with the data, a work-related attack is a very close second. It is just as important to critically examine the inconsistent for the most likely hypotheses as well. If there are many inconsistencies associated with the most likely hypotheses, this could signal that there is a missing hypothesis. However, if the inconsistent evidence can be refuted, then it can be regarded as "squishily" inconsistent, and the hypothesis probably is the most likely explanation.

Step 7: Analyze the sensitivity of your tentative conclusion to a change in the interpretation of a few critical items of evidence by using the software to sort the evidence by diagnosticity.

All of the hypotheses will include at least some inconsistent data. The goal of this step is to understand which pieces of evidence have the most overall effect on the relative likelihood of the hypotheses and what could happen if those pieces of evidence change.

When sorted by diagnosticity, it becomes apparent that some of the most potentially diagnostic pieces of evidence are already sources of controversy. For example, Walp said that he saw no signs of defensive wounds. By itself, this is a highly diagnostic piece of evidence because it is consistent with suicide, but it is inconsistent with the other hypotheses. While we should have fairly high confidence in this firsthand reporting, several law enforcement sources have reported that Luna did suffer defensive wounds as well as signs of restraint. As a result, this critical piece of evidence deserves further scrutiny.

Thomas DiBiagio's public comment that Luna was not in danger of losing his job is another diagnostic piece of evidence because it is highly inconsistent with both suicide hypotheses and fairly inconsistent with a work-related

attack by an adversary. However, separate reporting cites inside sources saying that DiBiagio had lied about Luna's work status to protect Luna's family. If, however, DiBiagio's public and alleged private comments are removed from the matrix, the suicide hypotheses remain the most inconsistent with the data. As a result, this piece of evidence is not as crucial as initially thought, because while DiBiagio's comments are highly applicable to the suicide hypotheses, they are not applicable to the other, more likely hypotheses.

Another piece of highly diagnostic evidence is the FBI's statement that Luna was alone all night. For the purposes of the ACH matrix, this "evidence" can be treated as an assumption. If it is assumed that this is true, it becomes a critical piece of evidence because it is highly inconsistent with all of the hypotheses except suicide. As a result, it is important to track down the underlying evidence that would support this assumption. The FBI did not make this evidence public, so analysts should consider what indicators would raise or lower their confidence in the veracity of this assumption.

Continue this process until all diagnostic evidence is reviewed.

Step 8: Report the conclusions by considering the relative likelihood of all the hypotheses.

The sensitivity analysis reveals areas for further scrutiny, but in the absence of additional information, the tentative conclusions about the relative likelihood of the hypotheses hold. However, any written analysis should include a full accounting of conflicting information, gaps, and assumptions upon which the analysis is based and what new information might change the likelihood of the hypotheses.

Step 9: Identify indicators or milestones for future observation.

The ACH process suggests that analysts should pay careful attention to new information that either corroborates or discredits Coronor Walp's assessment, the FBI's assertion that Luna was alone, or information about blood from a second person in the car. These pieces of information would differentiate further between the suicide and other hypotheses. Information about possible work-related problems, adversaries, recent contacts, extramarital activities, and previous threats could serve as important evidence that would discriminate between the lover and work-related hypotheses. These pieces of information could significantly affect the likelihood of the hypotheses and should therefore be targeted as key areas for further investigation in any future collection plan.

Analytic Value Added: **As a result of your analysis, what are the most and least likely hypotheses?** Work-related suicide and accidental suicide are the least likely hypotheses. A random attack is as unlikely as accidental suicide. The hypotheses that are least inconsistent with the relevant information are the jealous lover and work related attack.

What are the most diagnostic pieces of information? In addition to the diagnostic evidence discussed above, the alleged injuries to Luna's genitals, allegations that FBI mishandled a key informant, the possibility that there was blood of a second person in the car, and the fact that Luna was killed by his own penknife are most diagnostic.

What, if any, assumptions underlie the data? There is an implicit assumption that Walp and the FBI's public statements are highly credible sources of information and that they are more credible than the numerous law enforcement sources cited in the press reports.

Are there any gaps in the relevant information that could affect your confidence? Lack of information about the coroner's report, the basis for the FBI's assertion that Luna was alone, any known Luna adversaries or extramarital relationships, and the details of his financial situation constitutes important gaps that could affect overall confidence levels.

How confident are you in your assessment of the most likely hypothesis? Given the extensive gaps and contradictions in the evidentiary base, any assessment should include a low overall confidence level. However, analysts should have higher confidence that their analytic process has illuminated key areas for future research and collection.

Why do you think that the case remains unsolved? While it is impossible to know with certainty why the case remains unsolved, significant evidentiary gaps, anomalies, and uncertainties as captured in the public record most likely have played a role.

KEY TAKEAWAYS

- Write it down! When contradictory evidence is present, it is essential to review key assumptions and the reliability of all the data. Stand back and ask, Why?
- Consider a full range of hypotheses against all the

evidence and return to this analysis over time. There could be several, intertwined explanations, or the hypothesis could change over time as more information comes to light. Be prepared to evaluate each piece of new information against all the possibilities.

NOTE

1. Eric Rich and Allan Lengel, "US Prosecutor's Death Still Puzzling," *Washington Post,* December 3, 2004, http://www.washingtonpost.com/wp-dyn/articles/A29745–2004Dec2.html.

Table 8.1 ▶ Case Snapshot: The Assassination of Benazir Bhutto		
Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Chronologies and Timelines	p. 56	Decomposition and Visualization
Mind Maps	p. 86	Decomposition and Visualization
Analysis of Competing Hypotheses	p. 181	Hypothesis Generation and Testing

8 The Assassination of Benazir Bhutto
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

Some controversy still surrounds the question of who was responsible for Benazir Bhutto's death. Many people had motives, and more than one person or group could easily have been plotting to kill her. When confronting a case in which a significant amount of information is unknown, the analyst should focus first on devising and executing a solid analytic process that frames the problem and brings order to the jumble of data points, assumptions, and gaps that form the case. In short, the analyst should focus first on defining an analytic process at the outset that will increase the chances that he or she will identify and incorporate emerging information to solve the puzzle in the future.

The initial controversy surrounding this case as well as the detailed information that is publicly available make the case a particularly good vehicle for showing how analytic techniques such as Timelines, Chronologies, Mind Maps, Hypothesis Generation, and Analysis of Competing Hypotheses can help analysts systematically sort, array, and analyze a dataset to bring a complex set of events into better, if not complete, focus. Lastly, as with all cases in which human, technical, and press reporting are used, the case highlights the importance of both sourcing and confidence levels in analysis, particularly when dealing with eyewitnesses, secondhand reporting, and statements that may be intended to obscure the truth or misguide the analyst.

TECHNIQUE 1: CHRONOLOGIES AND TIMELINES

Chronologies and Timelines are simple but useful tools that help order events sequentially; display the information graphically; and identify possible gaps, anomalies, or correlations. In addition, these techniques pull the analyst out of the evidentiary weeds to view a data set from a more strategic vantage point. The complex and contradictory data regarding this case make an annotated Timeline particularly useful in identifying key pieces of evidence, confidence levels in the reporting, and gaps in the information.

Task 1.

Create a Timeline of events surrounding Benazir Bhutto's death.

Step 1: Label the relevant information from the case narrative with the date and order in which it reportedly occurred. Consider how best to array the data along the Timeline. Can the information be organized by category?

There are many ways to construct a Timeline for this case study. A complete Timeline of the case should go back to at least 1977, when General Zia al Haq overthrew Zulfikar Ali Bhutto, began Islamicizing Pakistan, and started nurturing militant groups to advance the state's perceived interests in Afghanistan and India and inside Pakistan. It should include all of the events leading up to her assassination on 27 December 2007 as well as all subsequent reporting that focused on the cause of death. It would include all references to key policy positions taken by Benazir Bhutto, her family, and her close associates as well as the statements and activities of all her political rivals and enemies.

For the purposes of this exercise, however, it is more practical to confine the Timeline exercise to the day she was killed and the information that surfaced subsequent to her death that shed light on how she died. A key objective in creating the Timeline is to capture all the critical information

uncovered in the investigations. This new information should be reflected on the Timeline at the time it allegedly occurred. In some cases, it might be preferable to include a separate citation for when the information was reported. Doing so not only helps an analyst see events as they unfolded but also to understand when information became available. This allows analysts to look for any anomalies in the pattern of the reporting that might support a deception hypothesis.

The Timeline in Figure 8.2, excerpted from a longer Timeline of the case, illustrates how relevant information can be displayed along several parallel tracks illustrating four dimensions of the event: Bhutto's activities, the government's actions and statements, the actions of the attackers and the Taliban, and the role of the media.

Step 2: Review the Timeline by asking the following questions:

- Are there data gaps?

The key issue that emerges from the Timeline is the apparent dispute over what actually caused Bhutto's death. The Timeline helps analysts sort through this issue by allowing them to compare known facts with the various statements of government officials and others cited by the media. Most of the initial reporting stated that she died of gunshot wounds. In subsequent days, the government declared that the actual cause of death was a head trauma caused by a major explosion that went off near Bhutto's SUV. Many have argued that the government was too quick to clean up the crime site and that a more methodical search might have revealed additional critical items of evidence. Some controversy also erupted over whether one or more assassins were involved in the plot. The only reference to a second bomber was the speculation prompted by the release of a grainy video that showed a man with a white scarf standing just behind the purported gunman. No other reference to this man appears in the case, and the Scotland Yard investigators contended that only one gunman was involved, who detonated his explosive vest after firing several shots. In contrast, the intercepted communication indicates that the purported perpetrators, the Pakistani Taliban, had intended to engage up to five assassins in the plot. Lastly, some would question the husband's decision not to demand an autopsy, expecting that a proper autopsy could have revealed more information.

- Do the duration and sequence of events suggested by the data make sense?

Some might question whether the government's seemingly premature statements were intended to cover up its failure to provide adequate security or, possibly, even some connivance in the plot to kill Bhutto. Many cite the quick decision to hose down the crime scene as indicative of possible government complicity in the crime.

- Could any events outside the Timeline have influenced the activities?

Little is known about the activities and whereabouts of several of the potential assailants, especially those tied to the Taliban or al-Qaeda.

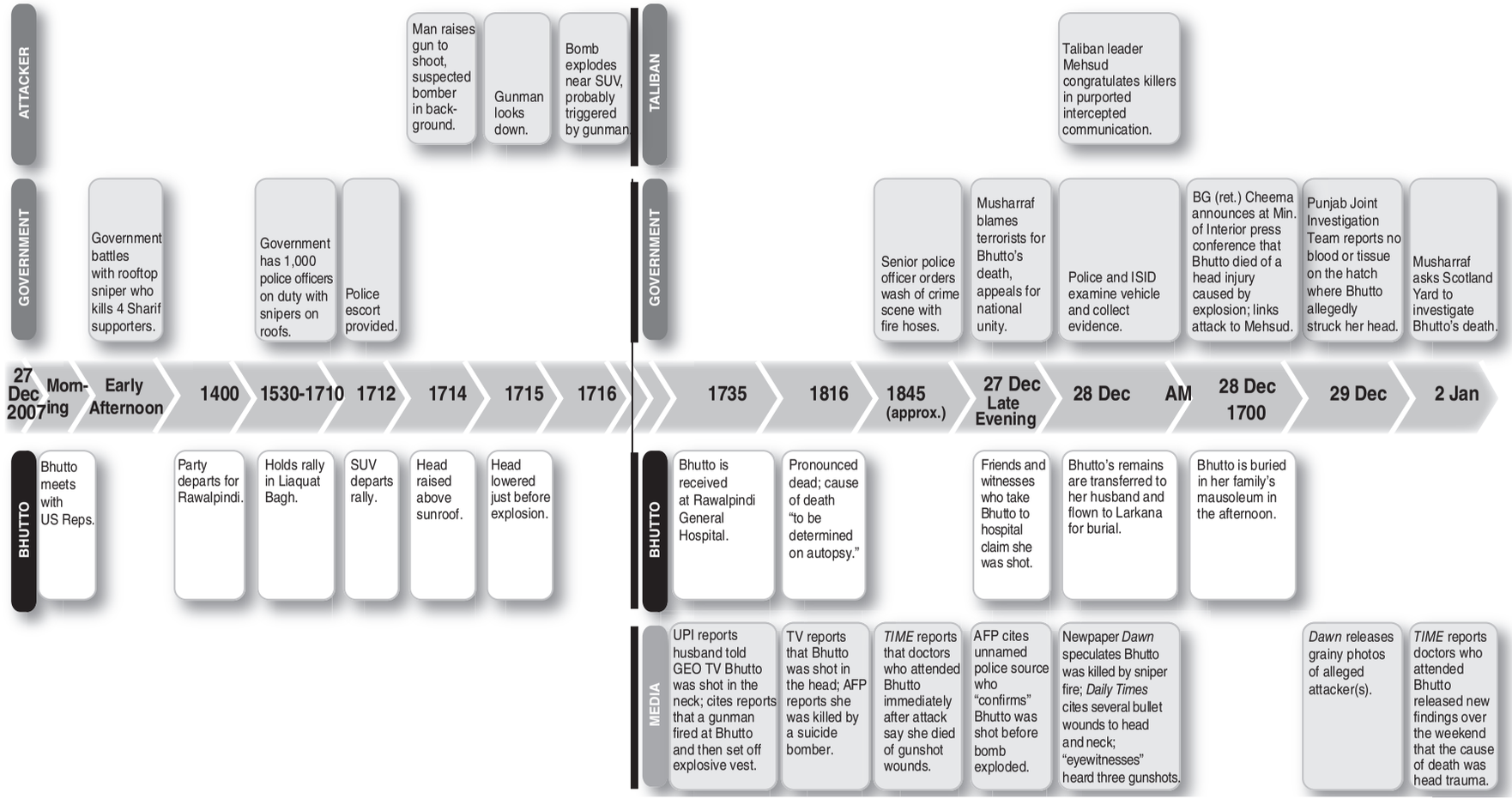
- Should any underlying assumptions about the evidence be taken into consideration?

The sources of information include eyewitnesses and confidential sources. For the purposes of the Timeline, we have segregated all the press reports as a separate stream of data. The government reporting also is presented as a separate stream of data because of the potential for bias in how it would cover the event. Sometimes when there are questions about the reliability of reporting or there are anomalies in the reports, analytic comment can be annotated on the report or the reports can be set off by a shaded box.

Analytic Value Added: **What does the sequence of events tell you?** The timeline helps the analyst distinguish between the various streams of information emanating from press sources, the government, and family friends. By isolating each stream of reporting, the analyst can better evaluate each. The timeline also illuminates the discrepancy between press reports that Bhutto died of a gunshot wound and subsequent government statements that the cause of death was a head trauma resulting from a nearby explosion. In addition, it calls out key data points for further investigation, such as the exact sequence of events just before the blast and the various accounts of what transpired.

Are there any gaps in the information that should be addressed? Several major gaps emerge, including the lack of information about the alleged attackers, confusion over whether just one or several attackers were involved, the identity or relevance of the man with a white scarf on the grainy video of the crowd, and the failure to learn more from an autopsy.

Figure 8.2 ▶ Timeline Excerpt: The Bhutto Assassination



Source: Pherson Associates, LLC, 2011.

What additional information should you seek? Key topics to pursue would include information on any plotting prior to the incident, any indications of government or ISID collusion with Baitullah Mehsud or other individuals who might target Bhutto, and any concrete evidence that the police were ordered to clean up the site prematurely.

How confident are you in the sources of information? The timeline suggests that careful scrutiny should be given to press reporting and eyewitness reports. In addition, the motives of all reporting sources should be evaluated with an eye toward determining if there was intent to deceive investigators or the public.

TECHNIQUE 2: MIND MAPS

Mind Maps are visual representations of how an individual or a group thinks about a topic of interest. A Mind Map diagram has two basic elements: the ideas that are judged relevant to whatever topic one is thinking about and the lines that show and briefly describe the connections between these ideas. Whenever you try to put a series of thoughts together, that series of thoughts can be represented visually with words or images connected by lines that represent the nature of the relationships between them. Any thinking for any purpose, whether about a personal decision or analysis of an intelligence issue, can be diagrammed in this manner. In fact, Mind Mapping was originally developed as a fast and efficient way for students to take notes during briefings and lectures.

In cases such as this, where initially there is little solid evidence and much speculation, it is particularly important to cast the net wide to make sure that nothing is excluded. This is especially so because the Pakistani government immediately leaped to a conclusion, blaming the so-called Pakistani Taliban operating in Pakistan's tribal belt. Although the hypothesis offered by the Pakistani government appears credible, the more important question is whether it is the only hypothesis worth considering.

Task 2.

Generate a Mind Map to explore who could have been behind Benazir Bhutto's assassination.

Step 1: Identify the focal question or the logical starting point for an investigation. Write the focal question down in the center of the page and draw a circle around it.

The focal question for this exercise is "Who was behind Benazir Bhutto's assassination?" The question "Who killed Benazir Bhutto?" would be inappropriate because the key question is who is the mastermind behind the killing, not who specifically pulled the trigger or exploded the bomb. With one possible exception—a lone-wolf scenario—the perpetrator(s) almost certainly was operating as an agent of a higher power.

Step 2: Brainstorm a list of possible explanations that might answer the focal question.

Step 3: Sort these ideas into groupings. These groups may be based on things they have in common or on their status as either direct or indirect causes of the matter being analyzed.

Step 4: Give each grouping a label and distribute these labels around the focal question. Draw lines from the focal question to each label.

Five groupings usually emerge in classroom discussions:

- The Pakistani government, including President Pervez Musharraf and senior officials in his government.
- Rival politicians.
- Islamic militants.
- Family members.
- Nation-states.

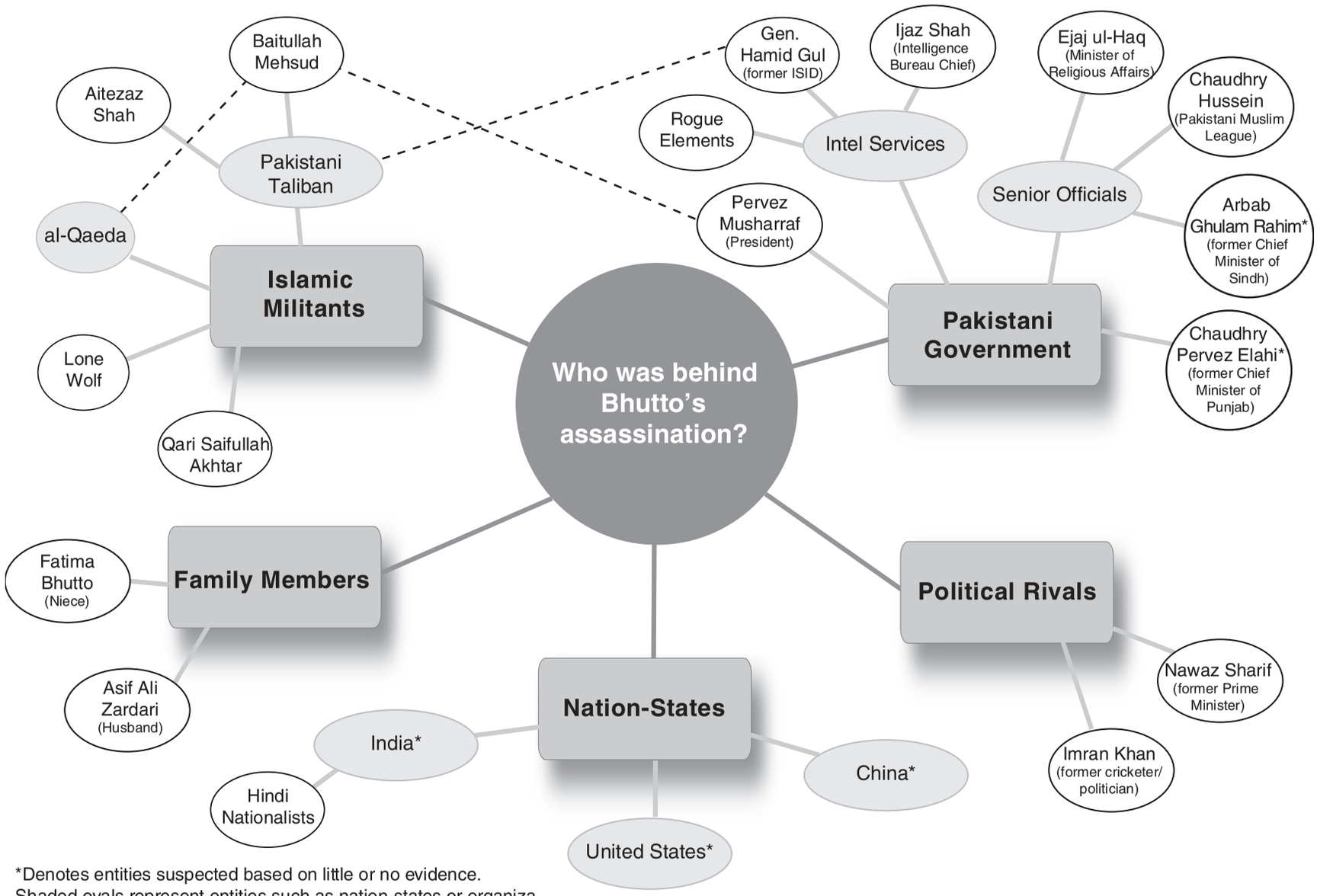
Step 5: For each label, draw a line to an issue or concept related to that label. A single label could have several spokes radiating from it, and each issue related to the label could have multiple spokes radiating from it as well.

Step 6: Continue to expand the diagram until all aspects of the issue or case have been captured.

As shown in Figure 8.3, the Mind Map is easier to read if different shapes and colors or shadings are used to show the various levels of hierarchy. In this case, the focal question is represented by a circle, categories by boxes, and specific entities and individuals by ovals. Different colors or shadings are also used to distinguish entities such as nation-states or organizations from individuals.

The focal question is presented in the circle as, Who was behind Bhutto's assassination? Five categories are depicted: Pakistani Government, Political Rivals, Nation-States, Family Members, and Islamic Militants. Each category has

Figure 8.3 ▶ Mind Map of Who Was Behind Bhutto's Assassination



*Denotes entities suspected based on little or no evidence.
Shaded ovals represent entities such as nation-states or organizations.

several entities and/or individuals associated with it. For example, two of Bhutto's relatives (her niece and husband) are connected to the Family Members category. The Pakistani government category is more complex, with one individual (President Musharraf) linked to it as well as two entities—Intelligence Services and Senior Officials. Each of these entities has several names associated with it, which can be extracted from the case study.

Step 7: While building the Mind Map, consider the possibility of cross-links from one issue to another. Show directionality with arrows pointing in one or both directions.

Several connections may be worth noting on the Mind Map, especially the link between President Musharraf and the Pakistani Taliban headed by Mehsud. The link between Pakistani Intelligence Chief Hamid Gul and the Taliban is also worth noting. These connections suggest that Mehsud could have acted either alone or with the support of the Pakistani government. Mehsud's links to al-Qaeda should be depicted as well, suggesting that this link could provide another reason for suspecting Mehsud. Lastly, Aitezaz Shah's reported links to the Pakistani Taliban require noting and possible further discussion.

Step 8: While building the Mind Map, consider the possibility of conflicting evidence or conflicting concepts. If they appear, label them differently by color, written name, or shape, or by putting an asterisk or other icon inside the circle or box.

In this case, it would be useful to color code linkages or hypotheses that could have been surfaced based on weak data or information that may have been provided with intent to deceive. Benazir Bhutto's message accusing four current and former Pakistani officials of having motive to kill her is not substantiated by any other information in the case. Similarly, a case can be made for nation-states such as India, China, or the United States being possible suspects given histories of past tensions, but such allegations are not substantiated by any information presented in the case study. It is a good idea to include such potential suspects in the Mind Map in order to generate a comprehensive list of suspects, but it is also helpful to indicate with color coding or an icon that the evidence supporting these suspects is weak.

Step 9: Reposition, refine, and expand the Mind Map structure as appropriate.

Once you have completed the Mind Map, take a final look to consider whether all the boxes and circles are arranged in the most effective way. For example, boxes connected by dotted lines should be in close proximity to each other. Sometimes, it is important to show the most important categories at the top of the Mind Map, where the reader's attention is most likely to focus first. In this Mind Map, both objectives were achieved by putting Islamic Militants and Pakistani Government at the top of the Mind Map.

Once the Mind Map is completed, the next task is to review all the options that have been generated and develop a list of alternative answers to the question, Who was behind the assassination of Benazir Bhutto? This is most efficiently accomplished by creating a table listing each branch of the Mind Map and assigning a motive to that person or group.

Step 10: List all the individuals or entities who may be behind the assassination as well as their most likely motivations.

See Table 8.2 for a list of potential masterminds and their motives. As a result of the Mind Map exercise, twenty-one individuals or groups have been identified.

Step 11: Identify the most likely people or entities that would have wanted to kill Benazir Bhutto.

Review the list of potential masterminds and select those with the strongest motives and the capability to orchestrate her assassination. A candidate list of five suspects provided in Table 8.3 includes the following:

- Pakistani Taliban leader Baitullah Mehsud, who allegedly authored the incriminating intercepted message praising one of his operatives for a successful attack.
- Pakistani President Pervez Musharraf, who could have viewed Bhutto's return and popularity as a threat to his regime.
- Former Prime Minister Nawaz Sharif, who was one of Bhutto's primary political challengers.
- Rogue elements of the ISID, who could have decided to take it upon themselves to remove a potential challenge to how they ran their business and how they related to other Islamic militant groups.
- Bhutto's niece, Fatima Bhutto, who held Benazir Bhutto responsible for her father's death and called Bhutto the most dangerous thing to happen to Pakistan.

Table 8.2 ▶ List of Potential Masterminds and Motives for the Bhutto Assassination

Individual or Entity	Possible Motive
Pakistani President Pervez Musharraf	Bhutto was a political rival who threatened his rule.
Rogue elements of the ISID	Bhutto's return to power would threaten their power and positions.
Former ISID Chief Hamid Gul	Bhutto believed he was plotting to kill her.
Intelligence Bureau Chief Ijaz Shah	Bhutto believed he was plotting to kill her.
Minister of Religious Affairs Ejaj ul-Haq	Saw Bhutto's return as unnecessarily destabilizing Pakistan.
Pakistani Muslim League leader Chaudhry Hussein	Strongly opposed any compromise with Bhutto.
Former Chief Minister of Sindh Arbab Ghulam Rahim	Bhutto believed he was plotting to kill her.
Former Chief Minister of Punjab Chaudhry Pervez Elahi	Bhutto believed he was plotting to kill her.
Former Prime Minister Nawaz Sharif	Bhutto was competing with him in the upcoming election.
Former politician Imran Khan	Had lambasted Bhutto in the press as a kleptocrat.
China	A Bhutto government could lead to a less-stable border and less-reliable partner.
United States	She was viewed as too anti-American or an unreliable future ally.
India	The return of a Bhutto government would resurface old tensions.
Hindu Nationalist Extremists	Her return posed a threat to all Hindus and to India.
Asif Ali Zardari (Bhutto's husband)	Her death could open political doors and protect him from corruption charges.
Fatima Bhutto (Bhutto's niece)	Fatima holds Bhutto responsible for her father's death.
Qari Saifullah Akhtar	Attempted a coup against her previously; suspect in October bombing.
Islamic militant lone wolf	She was viewed as too secular and female; an unacceptable Muslim.
al-Qaeda	She was viewed as too secular and too pro-American.
Pakistani Taliban leader Baitullah Mehsud	Saw Bhutto as too pro-American, too secular, and anti-Taliban.

Table 8.3 ▶ List of Most Likely Masterminds of the Bhutto Assassination

Most Likely Candidates	Possible Motive
Pakistani Taliban leader Baitullah Mehsud	Saw Bhutto as too pro-American, too secular, and anti-Taliban.
Pakistani President Pervez Musharraf	Bhutto was a political rival who threatened his rule.
Former Prime Minister Nawaz Sharif	Bhutto was competing with him in the upcoming election.
Rogue elements of the ISID	Bhutto's return to power would threaten their power and positions.
Fatima Bhutto (Bhutto's niece)	Fatima holds Bhutto responsible for her father's death.
Less Likely Candidates	**Possible Motive**
Islamic militant lone wolf	She was viewed as too secular and female; an unacceptable Muslim.
al-Qaeda	She was viewed as too secular and too pro-American.
Qari Saifullah Akhtar	Attempted a coup against her previously; suspect in October bombing.
Former ISID Chief Hamid Gul	Bhutto believed he was plotting to kill her.
Intelligence Bureau Chief Ijaz Shah	Bhutto believed he was plotting to kill her.
Mininster of Religious Affairs Ejaj ul-Haq	Saw Bhutto's return as unnecessarily destabilizing Pakistan.
Pakistani Muslim League leader Chaudhry Hussein	Strongly opposed any compromise with Bhutto.
Former Chief Minister of Sindh Arbab Ghulam Rahim	Bhutto believed he was plotting to kill her.
Former Chief Minister of Punjab Chaudhry Pervez Elahi	Bhutto believed he was plotting to kill her.
Former politician Imran Khan	Had lambasted Bhutto in the press as a kleptocrat.
Hindu Nationalist extremists	Her return posed a threat to all Hindus and to India.
Asif Ali Zardari (Bhutto's husband)	Her death could open political doors and protect him from corruption charges.
India	The return of a Bhutto government would resurface old tensions.
China	A Bhutto government could lead to a less-stable border and less-reliable ally.
United States	She was viewed as too anti-American or an unreliable future ally.

Analytic Value Added: **Does the creation of the Mind Map prompt you to consider a much broader array of potential explanations or hypotheses?** The act of drawing the Mind Map prompts analysts to think about a larger range of alternatives at the outset of a project. For example, once the analyst decides to list Fatima Bhutto as a potential mastermind, the question that immediately comes to mind is whether other family members, such as the husband, should be added to the Mind Map. The Mind Map approach also makes it easier to array a large number of alternatives in a simple display that is easy to embellish and refine.

Does it help you "drill down" for each hypothesis to consider second- and third-level questions? In this exercise, the Mind Map approach prompts the analyst to consider possible linkages between the groups and individuals depicted and to come up with the names of specific people who could have been the mastermind behind the operation. In considering the Islamic Militants category, for example, creating the Mind Map prompts one to explore several questions such as these:

- Which key Pakistani militant groups, such as the Harkat-ul-Jihad-al-Islami (HUJI), deserve attention, apart from the Pakistani Taliban?
- How are these various actors linked?
- Would they combine forces in an attempt to assassinate Bhutto?
- Did they have the capability to launch the attack that killed Bhutto?

Does it help you identify potential gaps in knowledge? The Mind Map approach not only reveals key gaps in knowledge but helps open the door to considering the possibility that several entities might simultaneously have been attempting to kill Bhutto and that more than one plot may have been playing out at the time of her death.

TECHNIQUE 3: ANALYSIS OF COMPETING HYPOTHESES

Analysts face a perennial challenge of working with incomplete, ambiguous, anomalous, and sometimes deceptive data. In addition, strict time constraints and the need to "make a call" often conspire with a number of natural human cognitive tendencies to result in inaccurate or incomplete judgments. Analysis of Competing Hypotheses (ACH) improves the analyst's chances of overcoming these challenges by requiring the analyst to identify and refute possible hypotheses using the full range of data, assumptions, and gaps that are pertinent to the problem at hand.

Task 3.

Use the most credible hypotheses compiled with the Mind Map or other hypothesis generation techniques to conduct an Analysis of Competing Hypotheses of the Bhutto case. Contact Globalytica, LLC at THINKSuite@globalytica.com or go to http://www.globalytica.com to obtain access to the basic software, or the collaborative version called Te@mACH®, if it is not available on your system.

Step 1: List the hypotheses to be considered, striving for mutual exclusivity.

The Mind Map technique can provide a useful starting point for generating a set of hypotheses. In the Mind Map, almost twenty groups or individuals were identified as suspects who may have given the order to have Benazir Bhutto killed. Lead the class in a discussion of all the possible motives for each entity and then choose those hypotheses that appear to be the most compelling and worthy of serious consideration. In this case study, the lead hypotheses that usually emerge are as follows:

- The Pakistani government (to include President Musharraf and other senior officials).
- The Pakistani Taliban (to include its leader, Baitullah Mehsud).
- Political rivals (specifically Nawaz Sharif, Bhutto's chief rival on the campaign trail).
- Rogue elements of ISID (who may not be acting on the specific orders of their leaders).

In class exercises, it usually is effective to include at least one other, less compelling hypothesis, such as one of Bhutto's family members, in order to illustrate the power of the ACH tool. Including a less likely suspect usually will result in generating a large number of inconsistent scores for that hypothesis, thereby showing how ACH illuminates the weakness of a poorly substantiated hypothesis.

Step 2: Make a list of all relevant information, including significant evidence, arguments, gaps, and assumptions.

Step 3: Assess the relevant information against each hypothesis by asking, "Is this information highly inconsistent,

inconsistent, neutral, not applicable, consistent, or highly consistent vis-à-vis the hypothesis?" The Te@mACH® software does not include the "neutral" category.

Step 4: Rate the credibility of each item of relevant information.

Figure 8.4 provides a partial list of fifty items of relevant information culled from the case study that could be helpful in conducting an ACH. Each of the items was assessed on a 5-point scale as Highly Consistent, Consistent, Inconsistent, Highly Inconsistent, or Not Applicable for each of the five candidate hypotheses.

In reviewing the completed matrix, it is noteworthy that almost half of the items of relevant information have little diagnostic value: they were rated as consistent or not applicable for all five hypotheses. Five, however, emerged as highly diagnostic because they were consistent with one hypothesis and inconsistent or highly inconsistent with the other four hypotheses. Two of the five items of relevant information were deemed highly diagnostic primarily because it was assumed that the other masterminds would be unlikely to utilize a suicide bomber to kill Bhutto. A word of caution is appropriate in that all but one of the most diagnostic items of evidence were rated as having "medium" credibility. For example, the intercept was deemed highly diagnostic but should not overly influence the analysis until the authenticity of the intercept can be established.

Step 5: Refine the matrix by reconsidering the hypotheses. Does it make sense to combine two hypotheses, add a new hypothesis, or disaggregate an existing one?

Figure 8.4 ▶ Bhutto Analysis of Competing Hypotheses Sample Matrix

PARC ACH 2.0.3 [P:\SAT Case Study Book-Analysis in Action\Cases\Chapter 5 Bhutto\Chapter 5 Bhutto for CC

File Edit Matrix Options Learning Aids Help

Enter Hypothesis | Enter Evidence | Sort Evidence By: Diagnosticity | Type of Calculation: Inconsistency Score | Du

		H: 2	H: 3	H: 4	H: 5	H: 1
		Taliban leader Mehsud	Bhutto's niece Fatima	Political rival Sharif	Rogue ISID elements	Musharraf and his Government
	Inconsistency Score ⇨	-6	-10	-11	-17	-19
	Enter Evidence					
E40	Purported govt intercept of Taliban leader Mehsud congratulates killers	C C	I I	I I	I I	I I
E44	Teenager confesses he was one of five assassins in plan to kill Bhutto	C C	I	I	I	I I
E48	Scotland Yard says Bhutto died of head injury caused by bomb blast	C	I	I	I	I
E41	CIA director says Mehsud behind killing of Bhutto	C	I	I	I	I
E29	Two days later MININT says shooter missed and Bhutto died of head trauma from bomb explosion	C	I	I	I	I
E47	Gun tied to man living in town controlled by Mehsud	C	I	I	C	I
E32	Doctors subsequently endorse MININT version of event	C	I	I	I	C

The current set of five hypotheses are sufficiently distinct from each other to argue against combining any into a single hypothesis. Given the strength of the Taliban hypothesis, thought should be given to exploring whether other hypotheses from the Islamic Militants category should be considered, such as a lone wolf, HUJI, or an al-Qaeda operative.

Step 6: Draw tentative conclusions about the relative likelihood of each hypothesis. An inconsistency score will be calculated by the software; the hypothesis with the lowest inconsistency score is tentatively the most likely hypothesis. The one with the most inconsistencies is the least likely.

The two hypotheses with the highest inconsistency scores are "Rogue ISID elements" and "Musharraf and his government." Some of the most compelling arguments for discarding these hypotheses are the fact that a suicide bomber was employed, the government had provided heavy security, Bhutto had stopped short of attacking Musharraf directly, and up to this point most of the suicide bombings had been targeted at the ISID and the military. The primary reason for dismissing "Political Rival Sharif " and "Bhutto's Niece Fatima" is the finding that Bhutto was killed by a suicide bombing, not bullets from a gun. Neither Sharif nor Fatima are likely candidates to have used a suicide bomber.

Step 7: Analyze the sensitivity of your tentative conclusion to a change in the interpretation of a few critical items of evidence by using the software to sort the evidence by diagnosticity.

The analysis would change dramatically if it were determined that the intercepted communication or the teenager's confession was not authentic or if new evidence emerged that one of the other suspects was involved in a plot to assassinate Bhutto that day. Also of concern would be a finding that the Scotland Yard report included the caveat that restrictions placed on its investigation by the Pakistani government may have precluded it from conducting a thorough inquiry.

Step 8: Report the conclusions by considering the relative likelihood of all the hypotheses.

The ACH software automatically moves the hypothesis or hypotheses that are the most credible to the left side of the matrix. The least likely hypothesis will appear on the far right. The most credible hypotheses are those with the fewest items of relevant information that are inconsistent with that hypothesis. Hypotheses with a large number of inconsistent items of relevant information that appear compelling can be discarded, unless some of the items of information are later found to be deceptive or inaccurate.

In this case study, "Taliban leader Mehsud" appears as the most likely mastermind behind the assassination of Benazir Bhutto. Only six items of relevant information were noted as being inconsistent with this hypothesis, and three of those were given a credibility rating of "low." For example, former ISID Chief Gul's complaint that authorities hosed down the crime scene could be interpreted as self-serving and an attempt to make the Taliban look innocent. Of more concern is the fact that Scotland Yard concluded there was only one attacker and no other suspicious individuals in the crowd. This seems to contradict what was said in the purported intercepted communication in which Mehsud was told that three men were involved in the assassination. One possibility is that three men were involved in the planning but only one suicide bomber was sent to the rally.

Step 9: Identify indicators or milestones for future observation.

The case for proving that Mehsud was the mastermind of the Bhutto assassination would be strengthened if additional information surfaced over the course of the investigation showing the following:

- Detailed planning by the Taliban to use a suicide bomber to kill Bhutto.
- Evidence that Mehsud or the Taliban were planning an attack on 27 December.
- More convincing evidence linking Mehsud to the teenager.
- Evidence that Musharraf or ISID was committed to protecting Bhutto and making an extra effort to ensure her safety.

Analytic Value Added: **As a result of your analysis, what are the most and least likely hypotheses?** Based on the ACH analysis, the most credible hypothesis is that Mehsud was the mastermind behind the assassination of Benazir Bhutto. All the other hypotheses had a significantly larger number of inconsistent items of relevant information, making them much less likely. Although Mehsud emerges

as the most likely suspect, a case can be made that he represents a family of likely suspects—Islamic militants—and that other individuals and groups in this category also merit close scrutiny. This would suggest that a second ACH exercise be conducted to apply the evidence to al-Qaeda, Qari Suifullah Akhtar, and a possible lone-wolf Muslim extremist.

The hypotheses "Musharraf and his government" and "Rogue ISID elements" both had a large number of inconsistencies, making them the least likely hypotheses. In the Mind Map exercise, however, historical links were cited connecting the intelligence services and the Taliban leadership. While the ACH methodology makes a strong case to dismiss the theory of Pakistani officials orchestrating a suicide bombing to eliminate Bhutto, the case to dismiss them as suspects becomes weaker if an argument is made that Pakistani officials were either colluding with or encouraging Islamic extremists to kill Bhutto.

What are the most diagnostic pieces of information? The most diagnostic evidence is the intercepted communication and subsequent arrest of the teenager who claimed to be part of a group tasked with assassinating Bhutto. The most compelling logic for discounting the other hypotheses was the use of a suicide bomb; other suspects would have lacked the capability to recruit a suicide bomber and almost certainly would have opted to use a sniper or gunman.

What, if any, assumptions underlie the data? The most important assumption was that only Islamic militants would resort to using a suicide bomber to kill Bhutto. Another key assumption is that only one assassination scenario was in play. Bhutto was regarded as a serious threat by a wide array of actors, and it is possible more than one was trying to kill her on that day.

Are there any gaps in the relevant information that could affect your confidence? How confident are you in your assessment of the most likely hypothesis? The key gap is not knowing if the intercepted communication and the statements made by the teenager are authentic. Another gap is whether more than one attacker was present in the crowd at the time of the bombing.

CONCLUSION: THE UN REPORT

Continued interest in the assassination of Benazir Bhutto led the Pakistani government and the United Nations Security Council to ask the UN Secretary-General to appoint a Commission of Inquiry to look into the events surrounding the killing and its aftermath. The three-member commission conducted more than 250 interviews in Pakistan with government officials and private citizens who had knowledge of the assassination. The commission's investigative team also examined the Scotland Yard report and reviewed hundreds of documents, photographs, and other documentary material provided by Pakistani and British officials. Following are some of the key findings of the report, published on 30 March 2010:

> Ms. Bhutto's assassination could have been prevented if adequate security measures had been taken. . . . The federal government under General Musharraf . . . [was] not proactive in neutralizing [threats] and/or ensuring that the security provided was commensurate to those threats.[1]

> She died when a 15 and a half year-old suicide bomber detonated his explosives near her vehicle, [but] no one believes that this boy acted alone.[2]

> Ms. Naheed Khan recalled that immediately after she had heard the three gunshots, Ms. Bhutto fell down into the vehicle onto her lap. Ms. Khan said that she felt the impact of the explosion immediately thereafter. . . . Ms. Khan saw that Ms. Bhutto was not moving and saw that blood was also trickling from the ear.[3]

> Five persons were arrested by [Pakistani officials]: Aitezaz Shah, Sher Zehman, Husnain Gul, Mohamad Rafaqat, and Rasheed Ahmed. In addition, [Pakistani officials] charged Nasrullah, Abdullah, Baitullah Mehsud, and Maulvi Sahib as "proclaimed offenders." . . . The accused are alleged to have served as handlers and logistics supporters of the suicide bomber, or as persons who were knowledgeable about the plans to assassinate Ms. Bhutto.[4]

> The investigation into Ms. Bhutto's assassination, and those who died with her, lacked direction, was ineffective, and suffered from a lack of commitment to identify and bring all of the perpetrators to justice.[5]

> The [Joint Investigation Team] . . . did nothing to build a case against Mr. Mehsud, treating the contents of the intercept presented to the public by Brigadier Cheema as determinative of his culpability. AIG Majeed told the Commission that he saw no need to establish the authenticity of the intercept or the basis for its analysis, including the voice identification and the interpretation of the conversation as a reference to Ms. Bhutto's assassination.[6]

The UN report shed light on several key aspects of the investigation. It noted that no blood or tissue was found on the truck's escape hatch lever, drawing into question whether Bhutto had hit her head on the lever when she fell into the cab.[7] The report also dismissed reports that doctors had deliberately altered their initial findings that Bhutto had suffered gunshot injuries. More significant, the commission said it had not found any credible, new information showing that Bhutto had received bullet wounds.[8]

The report noted that numerous people may have wished Bhutto harm, including local jihadi groups, the Pakistan Taliban, al-Qaeda, and members of the Pakistani government and political elite.[9] After the Karachi attack, Bhutto's attorney said that he had received a handwritten letter from someone claiming to be the "head of suicide bombers and a friend of al-Qaeda" who threatened to assassinate Bhutto in a gruesome manner. An al-Qaeda spokesperson, Mustafa Abu al Yazid, had also claimed responsibility for her assassination in an interview with the *Asia Times Online*.[10]

According to the UN report, many senior Pakistani officials believed Baitullah Mehsud was part of a larger conspiracy to assassinate Bhutto, but the report observes that many of these same officials would have had a motive to eliminate Bhutto because they were threatened by the possibility of her regaining power.[11,12] The true story of Mehsud's involvement may never be known because he was killed in a drone attack in August 2009.[13]

The commission took the police to task for focusing the investigation on lower-level operatives and not exploring whether any higher-level officials may have been involved in the planning, financing, or execution of the assassination.[14] It attributed police reluctance in part to a concern that Pakistani intelligence services may have had a role in the assassination.[15]

KEY TAKEAWAYS

- The tendency to "plunge in" should always be tempered by a process designed to identify all the relevant information and evaluate all possible explanations.
- Chronologies and Timelines are invariably some of the best ways to begin an analysis; they not only help the analyst organize the data but can reveal key gaps, inconsistencies, and correlations in the data.
- Employing a more systematic process, such as a Mind Map, at the start of the investigation helps frame the issue. It also helps analysts identify a more comprehensive set of hypotheses early on.
- Consider a full range of hypotheses against all the relevant information and return to this analysis over time. There could be several, intertwined explanations, or the hypotheses could change over time as more information comes to light. Be prepared to evaluate each piece of new information against all the possibilities.

INSTRUCTOR'S READING LIST

Jones, Owen Bennett. *Pakistan: Eye of the Storm*. New Haven, CT: Yale University Press, 2009.

MacBrayne, John. "Scotland Yard Statement on Bhutto Report [press release]." *Wall Street Journal,* February 8, 2008. http://online.wsj.com/article/SB120246987508353681.html.

Rashid, Ahmed. *Descent into Chaos: The US and the Disaster in Pakistan, Afghanistan, and Central Asia*, paperback ed. New York: Penguin Books, 2009.

United Nations. *Report of the United Nations Commission of Inquiry into the Facts and Circumstances of the Assassination of Former Pakistani Prime Minister Mohtarma Benazir Bhutto*. March 30, 2010. http://www.un.org/News/dh/infocus/Pakistan/UN_Bhutto_Report_15April2010.pdf.

NOTES

1. United Nations, *Report of the United Nations Commission of Inquiry into the Facts and Circumstances of the Assassination of Former Pakistani Prime Minister Mohtarma Benazir Bhutto*, March 30, 2010, http://www.un.org/News/dh/infocus/Pakistan/UN_Bhutto_Report_15April2010.pdf, 2.
2. Ibid., 2.
3. Ibid., 28.
4. Ibid., 41.
5. Ibid., 2.
6. Ibid., 41.
7. Ibid., 40.
8. Ibid., 32–33.
9. Ibid., 3.
10. Ibid., 48.
11. Ibid., 50.
12. Ibid., 51.
13. Ibid., 41.
14. Ibid., 3.
15. Ibid.

Table 9.2 ▶ Case Snapshot: Death in the Southwest

Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Structured Brainstorming	p. 102	Idea Generation
Starbursting	p. 113	Idea Generation
Key Assumptions Check	p. 209	Assessment of Cause and Effect
Multiple Hypotheses Generator™	p. 173	Hypothesis Generation and Testing
Analysis of Competing Hypotheses	p. 181	Hypothesis Generation and Testing

9 Death in the Southwest
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

This case study puts students in the shoes of Centers for Disease Control (CDC) investigators and local medical authorities who are under extreme pressure to determine why seemingly healthy people are suddenly dying. Although the instructional materials provide a detailed conclusion outlining how the case was actually resolved, much of this information was excluded from the narrative to give the students a better appreciation of how often analysts must make difficult judgments with relatively little solid data in hand. The Structured Brainstorming exercise is designed to prompt the students to consider all possible alternatives at the outset of a case, no matter how unrealistic they might appear at the time. The Starbursting exercise helps them transition from a divergent mode of analysis to a convergent mode by organizing and structuring the results of their brainstorming. The Multiple Hypotheses Generator™ provides a more systematic way to generate alternative hypotheses. Of the three techniques, the Multiple Hypotheses Generator™ probably does the best job of ensuring that the alternative hypotheses are mutually exclusive.

After reading the narrative, students usually are quick to articulate what they think is the most likely solution. The Key Assumptions Check and the Analysis of Competing Hypotheses (ACH) both prompt the analyst to subject their views to more critical scrutiny. The Key Assumptions Check forces the analysts explicitly to list their assumptions, some of which almost always turn out to be unfounded. Analysis of Competing Hypotheses requires analysts to consider an array of possible alternative hypotheses and then systematically evaluate which is the most likely based on whether the relevant information presented in the narrative is consistent or inconsistent with each hypothesis.

TECHNIQUE 1: STRUCTURED BRAINSTORMING

Brainstorming is a group process that follows specific rules and procedures designed to generate new ideas and concepts. The stimulus for creativity comes from two or more analysts bouncing ideas off each other. A brainstorming session usually exposes an analyst to a greater range of ideas and perspectives than the analyst could generate alone, and this broadening of views typically results in a better analytic product.

Structured Brainstorming is a systematic twelve-step process (described following) for conducting group brainstorming. It requires a facilitator, in part because participants are not allowed to talk during the brainstorming session. Structured Brainstorming is most often used to identify key drivers or all the forces and factors that may come into play in a given situation.

Task 1.

Conduct a Structured Brainstorming exercise to explore why a healthy young Navajo couple died suddenly.

Step 1: Gather a group of analysts with some knowledge of medicine and the Four Corners region.

It is helpful to include in the brainstorming group both experts on the topic and generalists who can provide more diverse perspectives. When only those directly involved with the issue are included, often the group tends to focus on the most current information gathered or the most readily available data; as a result, key assumptions remain unchallenged, and historical analogies can be ignored. In this case, having someone who understands Navajo culture and is familiar with both basic medical practice and the Four Corners area would be a major benefit.

Box 9.1 EIGHT RULES FOR SUCCESSFUL BRAINSTORMING

1. Be specific about the purpose and the topic of the brainstorming session.
2. Never criticize an idea, no matter how weird, unconventional, or improbable it might sound. Instead, try to figure out how the idea might be applied to the task at hand.
3. Allow only one conversation at a time and ensure that everyone has an opportunity to speak.
4. Allocate enough time to complete the brainstorming session.
5. Engage all participants in the discussion; sometimes this might require "silent brainstorming" techniques such as asking everyone to be quiet for five minutes and write down their key ideas on 3 × 5 cards and then discussing what everyone wrote down on their cards.
6. Try to include one or more "outsiders" in the group to avoid groupthink and stimulate divergent thinking. Recruit astute thinkers who do not share the same body of knowledge or perspective as other group members but have some familiarity with the topic.
7. Write it down! Track the discussion by using a whiteboard, an easel, or sticky notes.
8. Summarize key findings at the end of the session. Ask the participants to write down their key takeaway or the most important thing they learned on a 3 × 5 card as they depart the session. Then, prepare a short summary and distribute the list to the participants (who may add items to the list) and to others interested in the topic (including those who could not attend).

Step 2: Pass out sticky notes and marker-type pens or markers to all participants. Inform the team that there is no talking during the sticky notes portion of the brainstorming exercise.

Use different color sticky notes and encourage the participants to write down short phrases consisting of three to five words, not long sentences.

Step 3: Present the team with the following question: What are all the forces and factors that might explain why a young Navajo couple died suddenly?

Keep the question as general as possible so as not to inadvertently restrict the creative brainstorming process. It also helps to ask the group if they understand the question and whether they believe it should be worded differently. Spending a few minutes to ensure that everyone understands what the question means is always a good investment. Students should have the case study at hand for quick reference.

Step 4: Ask the group to write down responses to the question with a few key words that will fit on a sticky note. After a response is written down, the participant gives it to the facilitator, who then reads it aloud. Marker-type or felt-tip pens are used so that people can easily see what is written on the sticky notes later in the exercise.

Go around the room and collect the sticky notes. Give the students a few minutes to think about the issue and jot down a few ideas before you start reading out the responses. Read the responses slowly and stick them on the wall or the whiteboard in random order as you read them. Some sample sticky notes might read or address topics such as these: Is the disease contagious? Who else is getting sick? Have these symptoms been observed previously? Did the couple engage in patterns of activity that are common to other victims? Did the couple and other known victims visit the same location? Are there reports of toxic chemical dumps in the region? Are farmers using any new herbicides or other newly introduced chemicals? Did terrorists do it? Was it a hate crime? Who might want this to happen?

Step 5: Place all the sticky notes on a wall randomly as they are called out. Treat all ideas the same. Encourage participants to build on one another's ideas.

Step 6: Usually an initial spurt of ideas is followed by pauses as participants contemplate the question. After five or ten minutes there is often a long pause of a minute or so. This slowing down suggests that the group has "emptied the barrel of the obvious" and is now on the verge of coming up with some fresh insights and ideas. Do not talk during this pause, even if the silence is uncomfortable.

Remind the group not to talk during this part of the exercise. It is important for them to hear what others are suggesting, as this might stimulate new ideas for them to jot down. Also take care not to talk too much yourself. The participants need quiet time to think, and it is very important for the instructor not to interrupt their thought processes. Often when it is the quietest, the best thinking is taking place.

Step 7: After two or three long pauses, conclude this divergent thinking phase of the brainstorming session.

Step 8: Ask all participants (or a small group) to go up to the wall and rearrange the sticky notes by affinity groups (groups that have some common characteristics). Some sticky notes may be moved several times, and some may be copied if the idea applies to more than one affinity group.

If only a subset of the group goes to the wall to rearrange the sticky notes, then ask those who are remaining in their seats to form into small groups and come up with a list of key dimensions of the problem or key areas for more research based on the themes they heard emerge when the instructor was reading out the sticky notes. This keeps everyone busy and provides a useful check on what is generated by those working at the wall.

Step 9: When all sticky notes have been arranged, ask the group to select a word or phrase that best describes each grouping.

Four or five themes usually emerge from this part of the exercise.

- **Exposure.** The couple (and other victims) came into contact with a toxic substance that caused their illness. Exposure could have been accidental or intentional, a one-time occurrence or over a prolonged period of time. For example, the victims may have worked at Fort Wingate and been exposed to a lethal chemical or biological substance.
- **Identity.** The couple became ill because they were Navajos, belonged to a particular tribal group, lived on a particular compound, or were members or associates of a criminal gang.
- **Victims.** The two young Navajos were victims of a plot launched by international terrorists, white supremacists, or some other extremist group. They might have been targeted personally or simply been at the wrong place at the wrong time.
- **Natural causes.** The couple succumbed to a naturally occurring pathogen or virus that was particularly lethal. A visitor might have recently brought the pathogen to the area from some other part of the world, or something in the local environment might have caused it to surface.

Step 10: Look for sticky notes that do not fit neatly into any of the groups. Consider whether such an outlier is useless noise or the germ of an idea that deserves further attention.

Often one or two "outlier" sticky notes are worth pointing out to the class because they provide a fresh perspective or suggest a potentially valuable new line of inquiry. Here are some examples:

- A sticky note that said "Fort Wingate" could prompt a robust discussion of ways that Fort Wingate could be relevant. Were biological or chemical weapons being built or stored at the fort? Were there any known toxic waste sites at the fort? Did the couple or their associates work at the fort? Were any known white supremacist groups active at the fort? If so, did they have a website? Did it contain information critical of the Navajo Nation?
- A sticky note that said "rats" could prompt questions such as, What types of rats were indigenous to Four Corners? What types of diseases were such rats known to carry? How do diseases get transmitted from rats to humans? Under what conditions do rats pose a greater threat to the human population?

Step 11: Assess what the group has accomplished. Can you identify four or five key factors or forces that might explain why the young Navajo couple died?

Work with the group to develop a consensus on three or four themes that emerge as the most important dimensions of this problem or potential explanations for why the couple died. Write the candidate explanations on the board. The themes that most often are generated by this stage of the exercise are the following:

- **Exposure to a toxic substance.** The couple came into contact with a toxic chemical or biological substance in their surroundings that made them ill.
- **Natural causes.** The couple was exposed to a new pathogen that had recently manifested itself in their environment, or they died of a particularly virulent type of flu.
- **Victims of an attack.** Terrorists or domestic extremists introduced a particularly virulent biological substance into the environment with the intent to terrorize the population, to cause deaths among Navajos, or to draw attention to Fort Wingate.

Step 12: Present the results, describing the key themes or dimensions of the problem that deserve investigation.

The group should end up with a set of three to five hypotheses that best explain why the young Navajo couple died suddenly. At this stage of the exercise, the hypotheses can be fairly general so as not to rule out a viable alternative. Some sample hypotheses include these:

- The couple came in contact with a highly toxic chemical or biological substance.
- The two young Navajos were the victims of a deliberate hate crime targeting the Navajo Nation.
- The two young Navajos were collateral damage in a terrorist plot that for the first time involved the use of biological weapons.
- The couple succumbed to a particularly virulent, naturally occurring pathogen.
- The two young people had other health problems that made them more susceptible to the common flu.

Analytic Value Added: **Did we explore all the possible forces and factors that could explain why the young Navajo couple died? Did our ideas group themselves into coherent affinity groups?** Structured Brainstorming is a powerful tool for generating a diverse number of ideas; it taps the expertise and past experiences of everyone in the group and gives them equal opportunity to provide their input. The requirement to place all the ideas into affinity groups forces the group to critically examine the underlying forces and factors that might have caused the deaths while avoiding the cognitive trap of "satisficing," wherein one generates a short list of ready answers to the question without any underlying rigor to the process.

The silent, structured brainstorming approach is a powerful technique to pull out new and often never previously considered ideas and concepts. It avoids the trap of deferring to the most knowledgeable person in the room by giving all participants an equal, but silent, opportunity to surface their ideas.

Did our ideas group themselves into coherent affinity groups? How did we treat outliers—that is, the sticky notes that seemed to belong in a group all by themselves? Did the outliers spark new lines of inquiry? Did the labels we generated for each group accurately capture the essence of that set of sticky notes? While conducting the structured brainstorming exercise, it is useful to note whether particularly useful and creative ideas are generated after long pauses when everyone is thinking; if this does occur, it is important to alert the entire group to the phenomenon. Placing like ideas into affinity groups can be a challenging task; asking those not at the whiteboard to come up with their own categories often provides a useful sanity check. Always be careful to give outlier ideas their due attention; they often will point to new lines of inquiry or dimensions not previously considered.

TECHNIQUE 2: STARBURSTING

Starbursting is a form of structured brainstorming that helps analysts generate as many questions as possible. It is particularly useful in developing a research project, but it can also help to elicit many questions and ideas to challenge conventional wisdom. This process allows the analyst to consider the issue at hand from many different perspectives, thereby increasing the chances that the analyst will uncover a heretofore unconsidered question or idea that will yield new analytic insights.

Task 2.

Construct a Starbursting diagram to explore the Who? What? How? When? Where? and Why? questions relating to the untimely death of a healthy young Navajo couple.

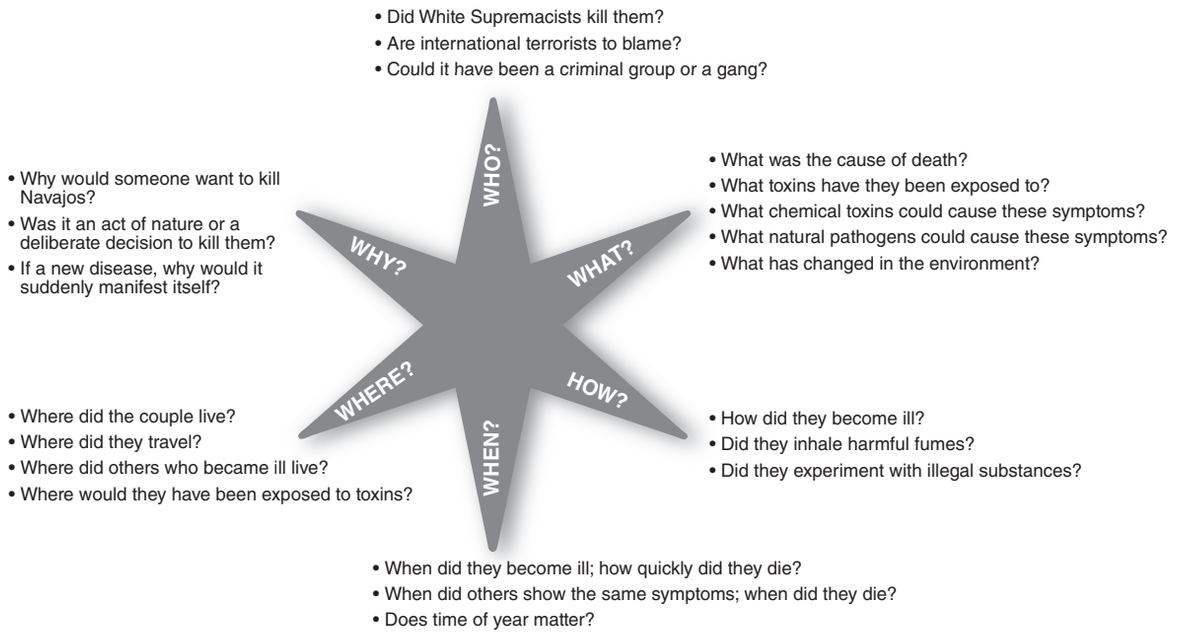
Step 1: Use the template in Figure 9.1 in the book or draw a six-pointed star and write one of the following words at each point of the star: *Who? What? How? When? Where?* and *Why?*

Step 2: Start the brainstorming session, using one of the words at a time to generate questions about the topic. Do not try to answer the questions during the brainstorming session; just focus on generating as many questions as possible.

Students should be able to develop at least two to four questions per "point" in the star, as reflected in example Figure 9.2.

Step 3: After generating questions that start with each of the six words, the group should either prioritize the questions to be answered or sort the questions into logical categories.

Figure 9.2 ▶ Death in the Southwest Starbursting Example



Depending on the specific questions they develop, students may choose to categorize the questions on the basis of the affinity groups they developed in the Structured Brainstorming exercise. In this case, possible pairings could include these:

- **What?** Can their deaths be attributed to exposure to a known transmitted disease; a new, naturally occurring pathogen; or a chemical toxin such as a new herbicide?
- **Who?** Might international terrorists, domestic extremists, or criminal elements have been responsible for their deaths?
- **Why?** Did they die because they were members of the Navajo Nation? Or because they belonged to some other group? Did they die as the result of natural causes or due to deliberate human acts?
- **Where?** Did where they live cause their death? Did they and other victims travel to the same place before becoming ill? Did something in the region make them ill or something at a specific location at Fort Wingate?

Another approach would be to organize the questions on the basis of a known factor, such as supporting evidence. For instance, they could form three groups of questions: one group of questions that have evidence to support the answer, another for which there is only indirect evidence or assumptions, and another for which there is no supporting evidence at all. Alternatively, students could prioritize the questions on the basis of known unknowns or gaps they seek to fill.

Analytic Value Added: As a result of your analysis, which questions or categories deserve further investigation? Analysts could focus their assessment on those questions that are most likely to move the investigation forward quickly either by eliminating potential hypotheses or further substantiating a lead hypothesis. For the example above, these might include the following:

- Are people who do not belong to the Navajo Nation dying as well?
- Are there any indications on the Internet that certain groups are targeting the Navajo Nation?
- What are the indications that the illness is contagious?
- What similarities can we detect among those who have become ill?

- Are there known toxic waste sites that all the victims might have visited?
- Are the symptoms consistent with any other viruses or diseases that are more lethal than the common flu?

TECHNIQUE 3: KEY ASSUMPTIONS CHECK

The Key Assumptions Check is a systematic effort to make explicit and question the assumptions that guide an analyst's interpretation of evidence and reasoning about any particular problem. Such assumptions are usually necessary and unavoidable as a means of filling gaps in the incomplete, ambiguous, and sometimes deceptive information with which the analyst must work. They are driven by the analyst's education, training, and experience, including the organizational context in which the analyst works. It can be difficult to identify assumptions, because many are sociocultural beliefs that are held unconsciously or so firmly that they are assumed to be truth and not subject to challenge. Nonetheless, identifying key assumptions and assessing the overall impact should conditions change are critical parts of a robust analytic process.

Task 3.

Conduct a Key Assumptions Check of the initial theory that the young Navajo couple died from a particularly virulent common flu virus.

Step 1: Gather a small group of individuals who are working the issue along with a few "outsiders." The primary analytic unit already is working from an established mental model, so the "outsiders" are needed to bring other perspectives.

In this instance, the Navajo tribal healers and experts from CDC in essence played the role of "outsiders." The historical perspective provided by the tribal healers turned out to be critical to solving the case.

Step 2: Ideally, participants should be asked to bring their list of assumptions when they come to the meeting. If not, start the meeting with a silent brainstorming session. Ask each participant to write down several assumptions on 3 × 5 cards.

Step 3: Collect the cards and list the assumptions on a whiteboard for all to see. A simple template can be used, as in Table 9.3.

In the early days of the investigation, much of the attention focused on the fact that almost all the victims were Navajos. Were they targeted because of their identity, did they frequent the same places, or did the illness have to do with where they lived? A key—and unwarranted—assumption early on was that the disease was contagious and might spread rapidly to other populations.

Step 4: Elicit additional assumptions. Work from the prevailing analytic line back to the key arguments that support it. Use various devices to prod participants' thinking. Ask the standard journalist questions: Who? What? How? When? Where? and Why? Phrases such as "will always," "will never," or "would have to be" suggest that an idea is not being challenged and perhaps should be. Phrases such as "based on" or "generally the case" usually suggest that a challengeable assumption is being made.

In this case, a key assumption deserving further investigation is that Fort Wingate may be the source of the problem because of its assumed involvement with the development of chemical and biological weapons. The challenge would be to establish a credible link between the facilities at Fort Wingate and the dead and sick people. Additional research also would be warranted to explore whether the recorded increase in the rodent population could be linked to the surge in sudden deaths. What diseases are rodents known to carry that would cause the symptoms reported of those who died? What would be required to transmit the disease from rodents to humans?

Table 9.3 ▶ Key Assumptions Check Template

Key Assumption	Commentary	Supported	With Caveat	Unsupported
1.				
2.				
3.				
4.				

Step 5: After identifying a full set of assumptions, critically examine each assumption. Ask:

- Why am I confident that this assumption is correct?
- In what circumstances might this assumption be untrue?
- Could this assumption have been true in the past but no longer be true today?
- How much confidence do I have that this assumption is valid?
- If this assumption turns out to be invalid, how much impact would it have on the analysis?

Step 6: Using Table 9.3, place each assumption in one of three categories:

- Basically supported
- Correct with some caveats
- Unsupported or questionable—the "key uncertainties"

Step 7: Refine the list, deleting those assumptions that do not hold up to scrutiny and adding new assumptions that emerge from the discussion.

In this instance, a final list of twelve key assumptions was generated. A critical examination of the list would place four assumptions in the Supported category, four in the With Caveats category, and four in the Unsupported category, as shown in Table 9.5. The Supported assumptions are supported by evidence reported by reputable sources—either doctors working the case or reports from well-respected research organizations. The assumptions With Caveats may well turn out to be correct, but there is insufficient evidence to prove they are true at this time. The assumption that the disease could spread quickly may be warranted at the outset of the investigation when public safety is a priority concern, but should not be used to justify

Table 9.5 ▶ Death in the Southwest Key Assumptions Check Example

Key Assumption	Commentary	Supported	With Caveats	Unsupported
1. Cause of death is a highly potent flu virus.	Symptoms are similar to those of flu, but flu strain would have to be unique to area.		✓	
2. Disease could spread quickly.	This is a genuine concern, but no evidence of spread beyond Four Corners.			✓
3. Disease has unusually high mortality rate.	Most of those who contract disease die within a few days.	✓		
4. The rapid deaths suggest a terrorist act.	There is no evidence that terrorists were targeting the Four Corners area.			✓
5. Illness can be treated with antibiotics.	Some treated did recover, but there is no proof recovery was due to antibiotics.		✓	
6. Most of the victims are Navajos.	The preponderance of those dying are members of the Navajo nation.	✓		
7. Navajos are being targeted.	There is no evidence that someone is intentionally targeting Navajos.			✓
8. Exposure to a toxic substance caused the deaths.	Many of the symptoms correlate with exposure to a toxic substance.		✓	
9. Dead Navajos were victims of a hate crime.	There is no evidence to support this.			✓
10. The disease is not contagious.	To date, no medical personnel have fallen ill from the disease.		✓	
11. Rodents are known carriers of disease.	Rodents are known carriers of many diseases with similar symptoms.	✓		
12. Rodent population grew tenfold 1992–93.	This fact has been documented by ecological researchers.	✓		

major resource decisions given the fact that caregivers are not coming down with the illness. The assumption that Navajos are deliberate targets is mere speculation unjustified by any known data.

Step 8: Consider whether key uncertainties should be converted into collection requirements or research topics.

The Key Assumptions Check should inspire the analysts to focus their attention on the Unsupported assumptions that have emerged as Key Uncertainties. Analysts could focus their assessment on those questions that are most likely to move the investigation forward. These might include the following:

- Are people who do not belong to the Navajo Nation dying as well?
- What are the indications that the illness is contagious?
- Are the symptoms consistent with any other viruses or diseases that are far more virulent than the common flu?
- Are there any reports of tourists contracting the disease or spreading it to other parts of the country when they return home?
- Are any Internet sites or blogs posting information critical of the Navajo Nation?
- What similarities can we detect among those who have become ill?
- Are there known toxic waste sites that all the victims might have visited?
- Can any link be established between Fort Wingate and those who have fallen ill or died of this disease?
- Can a link be established between a mushrooming rodent population and Navajos suddenly becoming ill? What would the tribal healers and history tell us about a potential link?

Analytic Value Added: **When CDC investigators arrived on the scene and interviewed doctors, did they inherit any key assumptions that would have had an impact on how effectively they organized their investigation?** CDC investigators were careful to review all the information provided by the on-site caregivers and to initiate new research to establish patterns and look for similarities. More important, they reached outside their normal circles to seek input from Navajo tribal healers in hopes of gaining additional perspectives on the case. This opened their minds to the possibility that they were dealing with a phenomenon that might have historical precedents; to wit, that the dramatic increase in the rodent population resulted in far greater rodent/human contact, allowing a particularly virulent disease to be transmitted to humans living in the area, most of whom were Navajos.

TECHNIQUE 4: MULTIPLE HYPOTHESIS GENERATION: MULTIPLE HYPOTHESES GENERATOR™

Multiple Hypothesis Generation is part of any rigorous analytic process because it helps the analyst avoid common pitfalls, such as coming to premature closure or being overly influenced by first impressions. Instead, it helps the analyst think broadly and creatively about a range of possibilities. The goal is to develop an exhaustive list of hypotheses, which can be scrutinized and tested over time against existing evidence and new data that may become available in the future.

The Multiple Hypotheses Generator™ is a useful tool for broadening the spectrum of plausible hypotheses. It is particularly helpful when there is a prevailing, but increasingly unconvincing, lead hypothesis—in this case, that healthy, young Navajos are dying from exposure to a virulent form of the common flu virus.

Task 4.

Use the Multiple Hypotheses Generator™ to create and assess alternative hypotheses that explain why the young Navajo couple died. Contact Globalytica, LLC at THINKSuite@globalytica.com or go to http://www.globalytica.com to obtain access to the Multiple Hypotheses Generator™ software if it is not available on your system.

Step 1: Identify the lead hypothesis and its component parts using Who? What? How? When? Where? and Why?

The lead hypothesis is this: "Healthy young Navajos are dying from exposure to a virulent form of the common flu virus." The key component parts are, Who (just Navajos or the population in general)? What caused them to become ill? How did they get ill? and possibly Where (was becoming ill associated with any particular facility or location)?

Steps 2 & 3: Identify plausible alternatives for the two or three most relevant key component parts and strive to keep them mutually exclusive. Discard any key component questions that one would consider to be "given" factors.

Two hypotheses could be generated in response to the Who question: just Navajos (because of shared identity, genetics, or specific Navajo Nation cultural practices) or anyone in the general population. Options for the What component could be the common flu, some other disease or natural pathogen, or a chemical toxin. The How component could be that the disease or toxin was present in the natural environment or that it was present because of human activity. In the latter case, someone could have deliberately exposed the victims to a biological or chemical agent, or the victims could have been exposed accidentally to a container or a location where chemical or biological toxins were present. In the former case, possible perpetrators could include domestic extremists, such as a white supremacist group, that deliberately wanted to target members of the Navajo Nation or international terrorists who wanted to incite terror among the general population. Accidental exposure could occur during the conduct of a tribal ceremony or because chemical or biological agents present at Fort Wingate were not being stored or handled properly.

The component When can be discarded because it is a given. The time frame is established as spring of 1993. Some students might choose to break down Why into categories such as "to incite terror" or "to kill Navajos," but such categories generally overlap with both How or What. We would recommend not using this component.

Table 9.6 shows the example output from the Multiple Hypotheses Generator™ for this lead hypothesis.

Table 9.6 ▶ Multiple Hypotheses Generator™: Death in the Southwest Alternative Hypotheses

Lead Hypothesis: Healthy young Navajos are dying from exposure to a virulent form of the common flu virus.

Components	Who?	What?	How?
Lead Hypothesis Components	Navajo	Virulent Form of the Common Flu	Act of Nature
Brainstormed Alternative Components	Anyone	Unknown Disease (Natural Pathogen)	Intentional Act of Man
		Chemical Toxin	Accidental Exposure

Step 4 & 5: Generate a list of possible permutations. Discard any permutations that simply make no sense.

The best way to array the various permutations is to create a permutation tree with multiple branches, as illustrated in Table 9.7. Once all the permutations are listed, it quickly becomes evident that several permutations can be dropped because they make no sense. For example, it makes no sense that only a subset of the population (e.g., members of the Navajo Nation) would be susceptible to the common flu. Similarly, if someone was intent on killing or terrorizing people, they would not pick the common flu as a weapon.

Step 6: Evaluate the credibility of the remaining permutations on a scale of 1 to 5, where 1 is low credibility and 5 is high credibility.

Two permutations that state that only Navajos are dying from a new pathogen or chemical toxin were not very likely but could not be ruled out entirely and thus received a rating of 1. For example, tribal healers could have unintentionally introduced a new and highly toxic substance into tribal ceremonies. Permutations that are slightly more credible were given a rating of 2. For example, it is possible—but not likely—that a naturally occurring chemical toxin had recently been exposed or had become present in some more virulent form, causing some people to die.

Permutations given ratings of 3 or above were deemed to have a more persuasive internal logic; if it turns out that they were correct, no one would be surprised. In this case, none of the permutations is so compelling that it received a rating of 5. It is important to note, however, that as more information becomes available, any of these ratings might be raised or lowered depending on what the new information reveals.

Step 7: Re-sort the remaining permutations, listing them from most to least credible, as shown in Table 9.8.

In this case study, the three permutations that received a rating of 4 and the three permutations that received a rating of 3 all deserve serious consideration. Several reasons can be given for assigning these permutations high ratings:

- The common flu kills thousands of people each year in the United States, and there have been past instances where a variant of the virus has caused an unusually high number of deaths.
- It is just as possible that some new form of a naturally occurring virus other than the common flu has broken out in the region and that a new pathogen is causing normally healthy people to die.
- There are multiple examples of radical extremists groups using biological agents to cause illness in the United States, as well as the celebrated case of a Japanese terrorist group, Aum Shinrikyo, dispersing sarin gas in the Tokyo subway system on 20 March 1995, causing hundreds of casualties.

Table 9.7 ▶ Multiple Hypotheses Generator™: Death in the Southwest Permutation Tree

Who?	What?	Why?	Permutations	Credibility Score
Only Navajos	Virulent Form of the Common Flu	Act of Nature	Only Navajos are dying from a virulent form of the common flu.	*discard*
		Intentional Act of Man	Someone is using a virulent form of the common flu to kill Navajos.	*discard*
		Accidental Exposure	Only Navajos are dying from accidental exposure to a virulent form of the common flu.	*discard*
	Unknown Disease (Natural Pathogen)	Act of Nature	Only Navajos are dying from a new, unknown natural pathogen.	1
		Intentional Act of Man	Someone is using a new, unknown natural pathogen to kill Navajos.	3
		Accidental Exposure	Only Navajos are dying from accidental exposure to a new, unknown natural pathogen.	*discard*
	Chemical Toxin	Act of Nature	Only Navajos are dying from a naturally occurring chemical toxin.	1
		Intentional Act of Man	Someone is using a chemical toxin to kill Navajos.	2
		Accidental Exposure	Only Navajos are dying from accidental exposure to a chemical toxin.	*discard*
Anyone	Virulent Form of the Common Flu	Act of Nature	People are dying from a virulent form of the common flu.	4
		Intentional Act of Man	Someone is using a virulent form of the common flu to kill people.	*discard*
		Accidental Exposure	People are dying from accidental exposure to a virulent form of the common flu.	*discard*
	Unknown Disease (Natural Pathogen)	Act of Nature	People are dying from a naturally occurring new, unknown pathogen.	4
		Intentional Act of Man	Someone is using a new, unknown pathogen to kill people.	4
		Accidental Exposure	People are dying from accidental exposure to a new, unknown natural pathogen.	3
	Chemical Toxin	Act of Nature	People are dying from a naturally occurring chemical toxin.	2
		Intentional Act of Man	Someone is using a chemical toxin to kill people.	2
		Accidental Exposure	People are dying from accidental exposure to a chemical toxin.	3

Slightly less credible would be these three possibilities:

- The history of the United States is replete with stories of hate crimes targeting minority populations. The use of a biological agent to target such people would not be surprising, particularly given recent history of a scientist sending anthrax through the mail to members of the US Congress and the media.
- The Four Corners region is largely rural, and it is possible that a new chemical substance or herbicide was recently introduced by farmers and is causing people to become ill and some to die.
- People in certain locations, possibly at Fort Wingate, have been accidentally exposed to a new and, for some, lethal form of a natural pathogen that is being developed or processed as part of a weaponization program.

Step 8: Restate the permutations as hypotheses.

The top six permutations could be restated as hypotheses in the following way:

- People in the Four Corners region are dying from a particularly virulent form of the common flu.
- People in the Four Corners region are dying from a naturally occurring, new, and still unknown natural pathogen.
- Someone (most likely international terrorists) is spreading a lethal biological pathogen to terrorize the population; similar attacks in other parts of the United States may be imminent.
- Someone (most likely a white supremacist group) is using a lethal biological agent like ricin or anthrax to kill members of the Navajo Nation.

Table 9.8 ▶ Multiple Hypotheses Generator™: Death in the Southwest Hypotheses Re-sorted by Credibility

Permutations	Credibility Score
People are dying from a virulent form of the common flu.	4
People are dying from a naturally occurring new, unknown pathogen.	4
Someone is using a new, unknown natural pathogen to kill people.	4
Someone is using a new, unknown natural pathogen to kill Navajos.	3
People are dying from accidental exposure to a new, unknown natural pathogen.	3
People are dying from accidental exposure to a chemical toxin.	3
Someone is using a chemical toxin to kill Navajos.	2
People are dying from a naturally occurring chemical toxin.	2
Someone is using a chemical toxin to kill people.	2
Only Navajos are dying from a naturally occurring chemical toxin.	1
Only Navajos are dying from a new, unknown natural pathogen.	1
Only Navajos are dying from a virulent form of the common flu.	*discard*
Someone is using a virulent form of the common flu to kill Navajos.	*discard*
Only Navajos are dying from accidental exposure to a virulent form of the common flu.	*discard*
Only Navajos are dying from accidental exposure to a new, unknown natural pathogen.	*discard*
Only Navajos are dying from accidental exposure to a chemical toxin.	*discard*
Someone is using a virulent form of the common flu to kill people.	*discard*
People are dying from accidental exposure to a virulent form of the common flu.	*discard*

- People who work at Fort Wingate have been accidentally exposed to a new, unknown natural pathogen.
- People living in the Navajo Nation have been accidentally exposed to a toxic chemical substance.

Step 9: Select from the top of the list those alternative hypotheses most deserving of attention and note why these hypotheses are most interesting (see Table 9.9).

Most of the symptoms manifested by those becoming sick or dying point to a naturally occurring disease as the most likely culprit. Although most of the victims are members of the Navajo Nation, other members of the general population also are dying. At this stage in the investigation, a key question is, What could have caused this new, natural pathogen to emerge? Is it a naturally occurring phenomenon, or was it intentionally introduced by someone to cause terror or to kill members of the Navajo Nation? The presence of Fort Wingate in the region also raises the possibility that people working there are being accidentally exposed to a lethal chemical or biological substance used in a weapons program at that facility.

Table 9.9 ▶ Multiple Hypotheses Generator™: Death in the Southwest Top Hypotheses

Top Hypotheses	Credibility Score
1. People are dying from a virulent form of the common flu.	4
2. People are dying from a naturally occurring new, unknown natural pathogen.	4
3. Someone is using a new, unknown natural pathogen to kill people.	4
4. Someone is using a new, unknown natural pathogen to kill Navajos.	3
5. People are dying from accidental exposure to a new, unknown natural pathogen.	3
6. People are dying from accidental exposure to a chemical toxin.	3

Analytic Value Added: **Which hypotheses should be explored further?** Additional medical tests should be conducted to help determine if a new virus might be the cause of the problem. Researchers also need to investigate how the victims acquired the pathogen. What commonalities exist in terms of where the victims worked, where they played, what locations they all might have frequented, or what work practices they might all share? If domestic radical extremists or terrorists were to blame, then research is needed to investigate why they would be targeting the Four Corners region or, more specifically, members of the Navajo Nation. For example, are there any recent postings on the Internet by such groups that would suggest that an attack on members of the Navajo Nation was justified? The chances that Fort Wingate is the source of the problem would be greatly increased if most of those who became ill worked at the fort or had relatives or acquaintances who worked there. Almost certainly, there would be press reports and a major "buzz" in the local community if Fort Wingate were the actual source of the problem.

Which of the six key components (Who? What? How? When? Where? and Why?) can be set aside because they are "givens," and why? The case study is challenging because many of the answers to these questions overlap. For example, the answer to Where? would indicate a natural cause if the Where turned out to be pastureland or farmland and, alternatively, an act of man if a specific location was identified that all the victims have frequented in recent weeks. The Why component poses similar challenges; at a minimum it focuses attention on what specific groups would have motive to launch an attack aimed at the Navajo Nation or the Four Corners region.

Which hypotheses from the original list were discarded, and why? Most of the hypotheses that were discarded were dropped because the internal logic of the permutation did not stand up to scrutiny. For example, a terrorist is not likely to use the common flu to cause a large-scale panic, nor would the use of the common flu be likely to generate large numbers of casualties.

TECHNIQUE 5: ANALYSIS OF COMPETING HYPOTHESES

Analysts face a perennial challenge of working with incomplete, ambiguous, anomalous, and sometimes deceptive data. In addition, strict time constraints on analysis and the need to "make a call" often conspire with a number of natural human cognitive tendencies to result in inaccurate or incomplete judgments. Analysis of Competing Hypotheses (ACH) improves the analyst's chances of overcoming these challenges by requiring the analyst to identify and refute possible hypotheses using the full range of data, assumptions, and gaps that are pertinent to the problem at hand.

Task 5.

Develop a set of hypotheses and use the Analysis of Competing Hypotheses software to identify which hypotheses provide the most credible explanation for the deaths in this case. Contact Globalytica, LLC at THINKSuite@globalytica.com or go to http://www.globalytica.com to obtain access to the basic software, or the collaborative version called Te@mACH®, if it is not available on your system.

Step 1: Generate a set of hypotheses to be considered based on what was learned from the Structured Brainstorming exercise, the Starbursting exercise, or the Multiple Hypotheses Generator™ exercise, striving for mutual exclusivity.

For the purposes of this illustration, the following four hypotheses were selected based on work done in previous exercises. It is recommended to include the initial lead hypothesis or the accepted common wisdom.

- Deaths are due to exposure to a particularly virulent common flu. (Common Flu)
- Deaths are due to accidental exposure to a toxic substance such as a chemical herbicide. (Toxic Substance)
- Navajos are the deliberate target of a hate crime. (Hate Crime)
- People are succumbing to a new pathogen—a mystery disease. (New Pathogen)

Step 2: Make a list of all relevant information, including significant evidence, arguments, gaps, and assumptions.

A careful reading of the narrative should generate fifteen to twenty items of evidence or relevant information that can be loaded on the software tool. Sixteen of the most important items of relevant information are listed in Figure 9.3.

Step 3: Assess the relevant information against each hypothesis by asking, "Is this information highly consistent, consistent, highly inconsistent, inconsistent, neutral, or not

Figure 9.3 ▶ Death in the Southwest ACH Evidence List

	Enter Evidence
E16	No reporting of anti-Navajo rhetoric on internet
E15	Recent wet winters and 10-fold increase in rodent population
E14	Powerful disease linked to wet winters and increased rodents
E13	Many died suddenly of similar powerful disease in 1918 & 1933
E12	Many symptoms consistent with presence of toxic substance
E11	Victims had abdominal/back pain with low blood platelet counts
E10	Surveys show not all had visited the same places
E9	Most patients live in Four Corners area
E8	Ft. Wingate munitions storage and demo facility nearby
E7	Some people treated with antibiotics recovered
E6	Tests for comon flu and bacterial agents are negative
E5	High mortality rate
E4	Young, healthy adults dying
E3	Almost all victims are Navajos
E2	Medical personnel are not becoming infected
E1	Victims have flu-like symptoms with quick progression to respiratory distress and death

applicable vis-à-vis the hypothesis?" (The Te@mACH® software does not include the "neutral" category.)

Analysts using the basic ACH software will have the option of choosing highly consistent (CC), consistent (C), inconsistent (I), highly inconsistent (II), not applicable (NA), or neutral (N). When using basic ACH or My Matrix with Te@mACH® tool, it is important that analysts code the evidence line by line, in other words horizontally across the matrix, not hypothesis by hypothesis, or vertically down the matrix. Doing so helps the analyst consider each piece of evidence fully against each hypothesis before moving on to the next piece of evidence. This process keeps the analyst focused on the evidence rather than on proving a pet hypothesis. The "Survey" option in Te@mACH® randomly generates the cells to be coded, thus avoiding this problem.

When entering and coding the data, the credibility score of all evidence or relevant information is set at a default of medium. Analysts can also choose a credibility score of low or high. The software in the basic ACH tool will calculate a weighted inconsistency score that reflects the analysts' judgment about credibility of the data.

With Te@mACH®, there is a special "Key Assumptions" box you can check to record and explain any key assumptions relating to a particular item of relevant information. In this case, one might want to note that for the item "Some people treated with antibiotics recovered," doctors could not prove that patients' recovery was directly connected to the use of antibiotics. The entry "Fort Wingate munitions storage and demo facility is nearby," also includes an implicit assumption that biological or chemical weapons are or were being processed at the fort and anyone working there could be exposed to toxic substances.

Step 4: Rate the credibility of each item of relevant information.

Step 5: Refine the matrix by reconsidering the hypotheses. Does it make sense to combine two hypotheses, add a new hypothesis, or disaggregate an existing one?

If the hypotheses are not mutually exclusive, this will become apparent at this stage in the process if the problem did not already surface during the coding process. Analysts should consider disaggregating hypotheses whenever they find themselves "clarifying" the hypothesis as they code. The trigger, or indicator, that disaggregation is necessary occurs during the coding process. For example, the hypothesis "Deliberate act by extremists," should be disaggregated to include one hypothesis for terrorists, who might want to target the general population, and a second hypothesis for white supremacists, who would only want to target Navajos or non-Caucasians.

Sometimes hypotheses can be disaggregated into a family of hypotheses. For example, exposure to a toxic substance could involve either a chemical or a biological substance. It could also involve an herbicide or some previously benign substance. It usually is more efficient to first address the overarching hypothesis. If this hypothesis seems likely, then a second ACH analysis can be created breaking the hypothesis into several mutually exclusive components. Similarly, if the hate-crime hypothesis emerges as a viable explanation, then serious consideration should be given to adding a terrorism hypothesis or a gang-warfare hypothesis.

Step 6: Draw tentative conclusions about the relative likelihood of each hypothesis. An inconsistency score will be calculated by the software; the hypothesis with the lowest inconsistency score is tentatively the most likely hypothesis. The one with the most inconsistencies is the least likely. The hypotheses with the lowest inconsistency scores appear on the left of the matrix, and those with the highest inconsistency scores appear on the right.

It is important to address the likelihood of every hypothesis, not simply the most and least likely. Based upon the above hypotheses and relevant information, some

tentative conclusions about the relative likelihood of each hypothesis would include the following observations:

- The "Common Flu" hypothesis is likely to have the most Inconsistents and is the easiest to dismiss.
- The "Hate Crime" hypothesis also has several Inconsistents and is not likely to be correct.
- The remaining two hypotheses have the fewest Inconsistents and appear worthy of serious consideration and further investigation.

It is just as important to critically examine the Inconsistent items of relevant information for the most likely hypotheses as well. If many Inconsistents are associated with all the most likely hypotheses, this could signal that there is a missing hypothesis. However, if the inconsistent evidence can be described at best as a "squishy" Inconsistent, then the hypothesis probably is the most likely explanation.

Step 7: Analyze the sensitivity of your tentative conclusion to a change in the interpretation of a few critical items of information, as shown in Figure 9.4. If using the basic ACH software, sort the evidence by diagnosticity, and the most diagnostic information will appear at the top of the matrix. The Te@mACH® software will automatically display the most diagnostic information at the top of the matrix.

All of the hypotheses will include at least some inconsistent data. The goal of this step is to understand which pieces of relevant information have the most overall effect on the relative likelihood of the hypotheses and what could happen if those pieces of evidence change.

Step 8: Report the conclusions by considering the relative likelihood of all the hypotheses.

The sensitivity analysis reveals areas for further investigation, but in the absence of additional information, the tentative conclusions about the relative likelihood of the hypotheses hold. However, any written analysis should

Figure 9.4 ▶ Death in the Southwest ACH Sorted by Diagnosticity

		H: 4	H: 2	H: 3	H: 1
		Navajos Succumb to New Pathogen	Exposure to Toxic Substance	Navajos Target of Hate Crime	Virulent Common Flu Virus
	Weighted Inconsistency Score ⇨	-1.0	-3.0	-5.0	-10.0
	Enter Evidence				
E6	Tests for comon flu and bacterial agents are negative	C	I	I	II
E11	Victims had abdominal/back pain with low blood platelet counts	CC	I	I	I
E7	Some people treated with antibiotics recovered	I	N	I	I
E16	No reporting of anti-Navajo rhetoric on internet	NA	N	II	NA
E10	Surveys show not all had visited the same places	N	I	N	I
E12	Many symptoms consistent with presence of toxic substance	N	CC	C	I
E4	Young, healthy adults dying	C	C	C	I
E3	Almost all victims are Navajos	C	C	CC	I
E2	Medical personnel are not becoming infected	C	C	C	I
E1	Victims have flu-like symptoms with quick progression to respiratory distress and death	C	C	C	I
E15	Recent wet winters and 10-fold increase in rodent population	C	NA	NA	N
E14	Powerful disease linked to wet winters and increased rodents	C	NA	NA	N
E13	Many died suddenly of similar powerful disease in 1918 & 1933	C	NA	NA	N
E9	Most patients live in Four Corners area	C	C	C	C
E8	Ft. Wingate munitions storage and demo facility nearby	N	CC	C	NA
E5	High mortality rate	C	C	C	C

include a full accounting of conflicting information, gaps, and assumptions upon which the analysis is based and what new information might change the likelihood of the hypotheses.

Step 9: Identify indicators or milestones for future observation.

The ACH process suggests that analysts should pay careful attention to new information that either corroborates or discredits the two lead hypotheses: New Pathogen or Toxic Substance. Critical questions for further investigation for the New Pathogen hypothesis include the following:

- What pathogens best match the symptoms that are being reported?
- Why do Navajos seem particularly susceptible to this new pathogen? What has changed in their environment to make them more susceptible or more exposed to a new pathogen?
- Do some rodents pose a particular threat? Are some known to carry a pathogen that could produce these symptoms? Are these rodents indigenous to areas populated by Navajos?

Critical questions for further investigation of the Toxic Substance hypothesis include the following:

- Have any new herbicides been introduced recently by farmers in the Four Corners area?
- Are there any toxic sites on the lands of the Navajo Nation that could be the cause of the problem?
- Did any of the victims work at Fort Wingate? Are there toxic dump sites at the fort, or are biological and/or chemical weapons being manufactured or stored there?

Analytic Value Added: **As a result of your analysis, what are the most and least likely hypotheses?** The two most likely hypotheses are that the people living in the Four Corners area were struck down by a new pathogen or recently exposed to a toxic substance.

What are the most diagnostic pieces of information? The most diagnostic items of information were the negative tests for flu, the specific symptoms of abdominal/back pain and low blood platelet counts, the lack of reporting of anti-Navajo rhetoric on the Internet, and the failure of care providers to come down with the same illness.

What, if any, assumptions underlie the data? At the start of the investigation, the CDC investigators were working from two key assumptions: that the cause of the sickness and deaths was either an unknown pathogen or a bioterrorist act. A corollary to the second assumption was that residents had been exposed to an unannounced or undetected biochemical spill at nearby Fort Wingate.

Are there any gaps in the relevant information that could affect your confidence? Many gaps remain in the evidence, as surfaced in the Starbursting and Key Assumptions exercises.

How confident are you in your assessment of the most likely hypotheses? We can be fairly certain that the cause of deaths was not the common flu and moderately confident that Navajos were not deliberately targeted for attack by terrorists or domestic extremists. More research is needed, however, before we can be confident that the cause of death was the introduction of a new pathogen or a recent, sudden exposure to a lethal chemical toxin.

CONCLUSION: THE ANSWER FROM ATLANTA

After a week of intense work, medical investigators concluded that the disease was not spreading through person-to-person contact, but they still had not yet identified its cause. On 4 June, CDC called with the results of tests they had run on the blood of the victims. They said the deaths were due to a "never-before-seen" strain of hantavirus. The hantavirus is named after the Hantaan River, which flows through North and South Korea, because it caused the illness and deaths of thousands of United Nations troops during the Korean War. Previously identified hantaviruses had caused kidney failure, but this newly identified strain was causing respiratory failure, and it was much more deadly.[1,2] A new viral hemorrhagic fever had been discovered in America.

Once medical investigators knew the cause of the illness, they turned to identifying the carrier of the virus and stopping its spread. CDC investigators immediately suspected, as with other hantaviruses, that the likely carrier was a rodent. Each hantavirus appears to "prefer" different rodents; the key question in this case was, "What rodent?" CDC provided the answer ten days later: the deer mouse.[3]

Even with the culprit identified, there were still many unanswered questions: How was the virus transmitted?

How long had the virus been present in the area? Tribal elders knew the presence of rodents in tribal homes put people at risk because it potentially exposed them to rodent feces and urine.[4] To avoid sickness, the elders recommended burning affected clothing and isolating food supplies. Tests on tissue samples collected and preserved by Sevilleta Wildlife Refuge ecologists showed that the now-termed "Sin Nombre" or "Without a Name" virus had been present in the rodent population for at least ten years before the 1993 epidemic. Based on the Navajo tribal healers' oral histories, epidemiologists suspected that rodent-transmitted disease had been present in the Four Corners Region since the early part of the twentieth century.[5]

In 1993, when precipitation plummeted—actually returned to normal—and available vegetative food sources were depleted, the increased rodent population began searching for food in new environments, such as barns and people's homes. The virus, which does not cause illness in the rodent host, was transferred from rodents to humans via saliva, urine, or fecal matter. Human infection occurs when the materials are inhaled as aerosols or introduced onto broken skin, similar to an anthrax infection. The disease was concentrated in the Navajo population simply because environmental conditions in the local area and agricultural cultivation increased contact between man and infected rodents. Visitors who had hiked or camped in the Navajo Nation area also became victims because of their exposure to the deer mouse.[6,7]

Research on the outbreak later determined that 50 percent of the infections were acquired in or around the home, 10 percent at the workplace, 5 percent during recreation, and the remainder for mixed or unknown reasons. A frequent antecedent of contracting the virus was opening and inhabiting a long unused cabin. This may be related to several factors: entry disturbs deer mice, which often urinate as they flee; the closed cabin lacks ventilation; and the roof prevents inactivation of the virus by the ultraviolet component of sunlight.[8]

Hantaviruses often bring death quickly. Usually 30 to 40 percent of patients die within twenty-four to forty-eight hours after admission to a hospital, even in well-run intensive care units (ICUs). The best indicator that a hantavirus is present is a finding of decreasing or abnormally low platelet counts. Approximately 40 percent of patients do not require the placement of a plastic tube into the trachea to protect the patient's airway and provide a means of mechanical ventilation. Treatment of the remainder of patients can be very challenging. Patients who survive, however, are often released in two to three weeks and usually show no major effects.[9]

THE FOLLOW-UP

Once the disease and the carrier were identified, public health officials advised local residents and visitors to the area to avoid activities that resulted in contact with wild rodents and to avoid disturbing rodent burrows to minimize the possibility of inhaling dried excreta. Homeowners who saw evidence of rodent infestation in their homes were encouraged to set traps; wash bedding; and don rubber gloves to wipe down countertops, cabinets, and walls with diluted bleach or disinfectant.

Since 1993, there have been a total of 560 cases of the virus in 32 states. About three-quarters of the infected people came from rural areas, with 63 percent of the reported cases being males. There is no treatment or effective cure.[10, 11]

KEY TAKEAWAYS

- It always pays to consider a broad range of alternatives before launching into a project or investigation.
- One of the first questions to ask at the start of a project or investigation is, What external expertise or external resources might I need to tap to perform my mission successfully?
- Consider a full range of hypotheses against all the relevant information and return to this analysis over time. There could be several, intertwined explanations, or the hypothesis could change as more information comes to light. Be prepared to evaluate each piece of new information against all the possibilities.

NOTES

1. David Perlin and Ann Cohen, "Hantavirus: Four Corners, United States," 2002, http://www.infoplease.com/cig/dangerous-diseases-epidemics/hantavirus-four-corners-united-states.html.

2. Tom Paulson, "Doctor on Trail of Another Deadly Virus," *Seattle Post-Intelligencer,* April 9, 2003, http://www.seattlepi.com/default/article/Doctor-on-trail-of-another-deadly-virus-1111862.php.

3. Centers for Disease Control, "Tracking a Mystery Disease: The Detailed Story of Hantavirus Pulmonary Syndrome (HPS)," updated May 17, 2011, http://www.cdc.gov/hantavirus/hps/history.html.

4. Linda Moon Stumpff, "Hantavirus and the Navajo Nation—A Double Jeopardy Disease," Evergreen State College, 2010, http://nativecases.evergreen.edu/collection/cases/hantavirus-navajo.html.

5. Ecological Society of America, "Ecological Research Benefits: The Hantavirus Case Study," http://www.esa.org/education_diversity/pdfDocs/hantavirus.pdf.

6. Perlin and Cohen, "Hantavirus: Four Corners, United States."

7. Ecological Society of America, "Ecological Research Benefits: The Hantavirus Case Study."

8. C. J. Peters and Ali S. Khan, "Hanta Pulmonary Syndrome: The New American Hemorrhagic Fever," *Clinical Infectious Diseases* 34 (2002): 1224–31, http://www2.medicine.wisc.edu/home/files/domfiles/infectiousdisease/Hantavirus.pdf.

9. Ibid.

10. Centers for Disease Control and Prevention, "Reported Cases of HPS," http://www.cdc.gov/hantavirus/surveillance/index.html (accessed June 14, 2011).

11. University of Wisconsin, "Scary New Diseases that Seem to Come Out of Nowhere," http://www.medmicro.wisc.edu/undergraduate/courses/554/pdf/scary_new_diseases.pdf (site discontinued).

Table 10.1 ▶ Case Snapshot: The Atlanta Olympics Bombing		
Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Key Assumptions Check	p. 209	Assessment of Cause and Effect
Pros-Cons-Faults-and-Fixes	p. 330	Decision Support
Multiple Hypotheses Generator™	p. 173	Hypothesis Generation and Testing

10 The Atlanta Olympics Bombing

Cases in Intelligence Analysis: Structured Analytic Techniques in Action

Instructor Materials

Police investigators were under severe pressure to discover who placed the bomb in Centennial Park and to bring that person or persons to justice. One person had been killed by the bomb and over a hundred were injured, and the public was justifiably concerned about safety at the Olympic Games. In such circumstances, the investigating team is under extreme pressure to come to closure quickly and to identify a prime suspect. Such dynamics make analysts and investigators vulnerable to groupthink and more likely to adopt satisficing strategies that will please all key stakeholders.

The best way to cope with such pressure is to employ structured techniques that allow investigators and analysts supporting them to take a few moments to reflect on what they know and what they need to know before plunging in to resolve the case. In this case study, we explore how three structured analytic techniques—the Key Assumptions Check, Pros-Cons-Faults-and-Fixes, and the Multiple Hypotheses Generator™—can be employed to better frame the problem and avoid going down unnecessarily time-consuming investigative blind alleys. Each technique takes relatively little time to employ—usually only an hour or two—but can save investigators much time over the long run by avoiding nonproductive leads. The techniques also can make the investigation more efficient by focusing attention on key information gaps and what types of additional information could prove the most compelling in helping to solve the case.

TECHNIQUE 1: KEY ASSUMPTIONS CHECK

The Key Assumptions Check is a systematic effort to make explicit and question the assumptions that guide an analyst's interpretation of evidence and reasoning about any particular problem. Such assumptions are usually necessary and unavoidable as a means of filling gaps in the incomplete, ambiguous, and sometimes deceptive information with which the analyst must work. They are driven by the analyst's education, training, and experience, including the organizational context in which the analyst works. It can be difficult to identify assumptions because many are sociocultural beliefs that are held unconsciously or so firmly that they are assumed to be true and not subject to challenge. Nonetheless, identifying key assumptions and assessing the overall impact should conditions change are critical parts of a robust analytic process.

Task 1.

Assume you are a member of the FBI team investigating the bombing. Piedmont College President Cleere has called the FBI office in Atlanta to present his rationale for making Richard Jewell a prime suspect in the case. Following consultations with Washington, D.C., your team has decided to do just that. To help kick off the investigation, you have been asked to conduct a Key Assumptions Check with your teammates to go over what assumptions the team is making about Jewell and the bombing in Centennial Park. Your task is to guide the team through the following eight steps for conducting a Key Assumptions Check.

Step 1: Gather a small group of individuals who are working the issue along with a few "outsiders." The primary analytic unit already is working from an established mental model, so the "outsiders" are needed to bring other perspectives.

In this case, the FBI team of investigators would benefit from including some local or state law enforcement officials in the brainstorming process.

Step 2: Ideally, participants should be asked to bring their lists of assumptions when they come to the meeting. If not, start the meeting with a silent brainstorming session. Ask each participant to write down several assumptions on a 3 × 5 card.

Step 3: Collect the cards and list the assumptions on a whiteboard for all to see. A simple template can be used, like the one shown in Table 10.2 in the book.

Step 4: Elicit additional assumptions. Work from the prevailing analytic line back to the key arguments that support it. Use various devices to prod participants' thinking. Ask the standard journalist questions: Who? What? How? When? Where? And Why? Phrases such as "will always," "will never," or "would have to be" suggest that an idea is not being challenged and perhaps should be. Phrases such as "based on" or "generally the case" usually suggest that a challengeable assumption is being made. A list of possible key assumptions is provided in Table 10.5.

Step 5: After identifying a full set of assumptions, critically examine each assumption. Ask:

- Why am I confident that this assumption is correct?
- In what circumstances might this assumption be untrue?

Table 10.5 ▶ Atlanta Olympics Bombing Key Assumptions Example

Key Assumption	Supported	With Caveats	Unsupported
1. The attack was a single incident involving one bomb.	✓		
2. Many more people would have died or been injured if Richard Jewell had not alerted authorities to the knapsack.	✓		
3. Jewell placed the 911 call.			✓
4. The bomb materials were readily available.	✓		
5. Jewell could have constructed the bomb.		✓	
6. Jewell would have known how to place the bomb without being seen.			✓
7. The bomb was intended to kill large numbers of people indiscriminately.		✓	
8. The bombing was not a political act.			✓
9. Jewell intended the bomb to explode in fewer than 30 minutes because his intent was to clear the area of people and ambush police and security officers.		✓	
10. Ray Cleere's statements were truthful and not motivated by his holding a grudge against Jewell.		✓	
11. Jewell had law enforcement or military training in bomb making.		✓	
12. Jewell wanted a job with the Atlanta police.	✓		
13. Jewell placed the bomb so he could become a hero.		✓	
14. Jewell's personality fit the profile of someone who would create an incident so he could emerge a hero.		✓	
15. Jewell's personality fit the profile because he sought out publicity after the bombing.			✓
16. Jewell might be the bomber because he appeared uncomfortable talking about the victims out of guilt.			✓
17. Jewell's statement that he wanted to get a position on the Atlanta police department was inappropriate and could indicate he had a motive for planting the bomb.			✓
18. Law enforcement officials were receiving daily bomb threats.	✓		

- Could this assumption have been true in the past but no longer be true today?
- How much confidence do I have that this assumption is valid?
- If this assumption turns out to be invalid, how much impact would it have on the analysis?

Many of the assumptions make sense when taken at face value but quickly fall apart when examined more closely. For example, several assumptions suggesting that Jewell's statements after the bombing indicated he might be the bomber are totally unsupported. Jewell had a legitimate reason to be looking for a job because he expected to be unemployed after the Olympics ended, and most of the press sought him out because he had a seemingly powerful story to tell of helping save many lives. The assumptions that he planted the bomb to create an incident to make him look like a hero can't be totally dismissed, however, given Jewell's rocky employment history and problems in previous law enforcement positions.

The assumption that Jewell placed the 911 call is unfounded because Jewell would have needed more time to get from Centennial Park to the Days Inn. While this argues convincingly against assuming Jewell made the phone call, it raises a different question: What if Jewell had an accomplice? The accomplice could have made the call, and the two perpetrators could have communicated with each other over cell phones.

Step 6: Using Table 10.2, place each assumption in one of three categories:

- Basically supported
- Correct with some caveats
- Unsupported or questionable—the "key uncertainties"

One technique you can employ to decide which category to assign to an assumption is to ask the questions: Can I make decisions about moving resources or people based on this assumption? If the answer is "yes" then the assumption can be rated as "supported." If the answer is "it depends," then the assumption merits a rating of "with caveats," and the caveat(s) needs to be recorded. If it would be inappropriate or hard to justify the movement of people or resources on the basis of this assumption, then the assumption is "unsupported."

In this case study, five of the assumptions appear solid, seven require caveats, and six of the key assumptions are unfounded. The assumption that the "bomb was intended to kill large numbers of people" is supported by the use of nails and shrapnel in the bomb construction; however, a credible alternative hypothesis is that Jewell's real intent was to minimize casualties and limit deaths to a small number of law enforcement and security officials because he made the warning call to 911. Other assumptions requiring caveats relate to whether Jewell was creating an incident in order to become a hero and to get a good job. While there is no direct evidence to support this assumption, Jewell's past problems working in law enforcement would argue that such a hypothesis is worthy of investigation.

A key question that usually arises from the exercise is, What motivated Cleere to make the call? If he had not called the FBI Atlanta Field Office to offer his theory, Jewell may have never risen to the status of a prime suspect. Cleere could have held a grudge against Jewell and made the call simply to get him in trouble with the authorities. At a minimum and pending further investigation, the assumption that Cleere was truthful should be considered with caveats. Finally, the assumption that Jewell had military or law enforcement training in bomb making is correct but should be considered with caveats because we do not know if the training was sufficient to teach him how to make the actual bomb that was used.

Step 7: Refine the list, deleting those assumptions that do not hold up to scrutiny and adding new assumptions that emerge from the discussion.

The assumption "Jewell placed the 911 call," would have to be dropped, given the time differences, or replaced by a new assumption that "An accomplice of Jewell placed the call." At a minimum, the discrepancy would argue for carefully reviewing and validating key segments of the chronology of events.

Step 8: Consider whether key uncertainties should be converted into investigative leads, collection requirements, or research topics.

The Key Assumptions Check suggests several new avenues for investigation. For example, an effort should be made to determine if Cleere could have had any ulterior motives in calling the FBI Atlanta Field Office to present his theory. Moreover, should we assume that Jewell acted alone, or could there have been several perpetrators? If the timing suggests that Jewell was primarily interested in killing police and security personnel, would the placement of the bomb support this theory as well? Would Jewell have known that

a large group of law enforcement officers would converge on the site fairly quickly? How would Jewell have acquired this information? Would this suggest that Jewell might have been surveilling the site for several days? If so, would such activity show up on the security video cameras? If so, wouldn't Jewell be concerned that the cameras would catch him planting the bomb? Would Jewell have known about the security cameras?

Analytic Value Added: What assumptions, if any, did law enforcement analysts and officials make as they began the investigation? Law enforcement officials fairly quickly focused on a single, lead hypothesis that Jewell had planted the bomb with the intent of revealing it to the authorities and taking credit for minimizing the number of casualties. They assumed motive and capability and, as new information surfaced, decided how it could be made to fit the lead hypothesis. Information inconsistent with this lead hypothesis, such as the impossibility of both making the 911 call and alerting authorities in Centennial Park to its presence one minute later, was ignored.

Were they influenced by key assumptions of others, including the press and the experts they interviewed, who wanted to assist their work? FBI investigators initially responded to the call from Piedmont College President Cleere, appropriately treating this hypothesis as worthy of further investigation, but nothing in the public record shows that they challenged the assumption that Cleere was truthful and not carrying a grudge against Jewell.

As colleagues generated other examples of the "wannabe hero" syndrome, however, they fell into the trap of "satisficing," whereby a proposed explanation or theory of the case quickly gains acceptance because it fits with most of the key facts and the explanation satisfies the needs of one's supervisors and the public.

Did the investigators fall into the trap of groupthink, or did they have sufficient cause to focus on Jewell as a suspect? The investigators quickly fell into the trap of groupthink, allowing a tip from President Cleere and a few anecdotes—of people having taken credit for incidents to make themselves appear as heroes—to dominate their thinking. In reviewing Jewell's past history in law enforcement, they were quick to confuse correlation with causality. Moreover, the case study notes that Jewell was charged with impersonating a police officer but does not reveal if he was actually convicted. Although Jewell had a history of employment problems, there was nothing in his case history to suggest that he would go to the extreme of constructing an antipersonnel bomb and exploding it at the Olympic Games.

What impact did key assumptions have on how effectively the FBI organized its investigation? If the investigators had critically examined all their key assumptions, asking themselves under what circumstances each assumption could turn out to be incorrect, they would have been less prone to jump to the conclusion that Jewell was the bomber. Conducting the Key Assumptions Check raises several additional questions that merit more serious attention: (1) "Should Jewell be considered the prime suspect if he could not have placed the phone call?" (2) "Wouldn't Jewell have had more prospects of success if he discovered a bomb that was yet to explode?" and, more generally, (3) "Was the bomber acting alone?"

TECHNIQUE 2: PROS-CONS-FAULTS-AND-FIXES

Pros-Cons-Faults-and-Fixes (PCFF) is a simple strategy for evaluating many types of decisions, including the decision to launch a police investigation. In this case, law enforcement officials are under substantial pressure to decide whether Richard Jewell was responsible for planting the bomb. PCFF is particularly well suited to situations in which decision makers must act quickly, because the technique helps to explicate and troubleshoot a decision in a quick and organized manner so that the decision can be shared and discussed by all decision-making participants.

Task 2.

Use PCFF to help you decide whether Richard Jewell was responsible for planting the bomb in Centennial Park, as shown in Table 10.6.

Step 1: Clearly define the proposed action or choice.

The question to address is "Did Richard Jewell plant the bomb in Centennial Park?"

Step 2: List all the Pros in favor of the decision. Think broadly and creatively and list as many benefits, advantages, or other positives as possible. Merge any overlapping Pros.

Step 3: List all the Cons or arguments against what is proposed. Review and consolidate the Cons. If two Cons are similar or overlapping, merge them to eliminate redundancy.

Table 10.6 ▶ Atlanta Olympics Bombing Pros and Cons Example

Question: Did Richard Jewell plant the bomb in Centennial Park?	
Pros	Cons
1. He alerted the police to the knapsack containing the bomb.	1. He could not have made 911 call and alerted police to the presence of the knapsack.
2. He enjoyed getting publicity.	2. He would not have treated other police officers as his prime target.
3. He had problems in past jobs and needed a future job.	3. He would not have constructed an antipersonnel bomb.
4. He had previous bomb training.	4. He had no reason to detonate the bomb early, before 30 minutes.
5. The bomb was crude.	5. There were no witnesses or any forensics linking him to the attack.

Step 4: Determine Fixes to neutralize as many Cons as possible. To do so, propose a modification of the Con that would significantly lower the risk of the Con being a problem, identify a preventive measure that would significantly reduce the chances of the Con being a problem, conduct contingency planning that includes a change of course if certain indicators are observed, or identify a need for further research or to collect information to confirm or refute the assumption that the Con is a problem.

Fixes can be generated for several of the Cons:

- He could not have made the 911 call and alerted police to the presence of the knapsack—Jewell had an accomplice.
- He would not have treated other police officers as his prime target—the more damage that was done, the more he could be portrayed as a hero.
- He would not have constructed an antipersonnel bomb—the more damage that was done, the more he could be portrayed as a hero.
- He had no reason to detonate the bomb early, before 30 minutes—it went off unintentionally.
- There were no witnesses or forensics linking him to the attack—he knew he might become a suspect and so was careful to avoid leaving any fingerprints behind.

Step 5: Fault the Pros. Identify a reason the Pro would not work or the benefit would not be received, pinpoint an undesirable side effect that might accompany the benefit, or note a need for further research to confirm or refute the assumption that the Pro will work or be beneficial.

Faults can also be generated for all of the Pros:

- He alerted the police to the knapsack containing the bomb—he was just doing his job as he was trained to do it.
- He enjoyed getting publicity—this did not become apparent until several interviews had been done and he realized how much fun it was to be an instant celebrity.
- He had problems in past jobs and needed a future job—there is no past history of him being involved in making bombs, espousing extreme views, or threatening to do violence.
- He had previous bomb training—this is frequently the case for most police officers.
- The bomb was crude—lots of people would have been just as capable as Jewell at making such a bomb.

Step 6: Compare the Pros, including any Faults, against the Cons and Fixes, as shown in Table 10.7.

On balance, the Cons appear to make a stronger statement than the Pros. Similarly, the Fixes for the Cons are relatively weak, and the Faults for the Pros present more convincing counterarguments. The fact that Jewell could not have made the 911 call and alerted police, given the timing of both events, is the most compelling factor. On further inspection, one could question whether a "wannabe hero" would have even bothered to make a phone call—especially one that would require using an accomplice and thereby forfeit personal control over a key part of the scenario. Similarly, the choice of an antipersonnel device is

Table 10.7 ▶ Atlanta Olympics Bombing Pros-Cons-Faults-and-Fixes Example

Faults	Pros	Cons	Fixes
Richard Jewell was doing his job.	He alerted the police to the knapsack containing the bomb.	He could not have made 911 call and alerted police to the presence of the knapsack.	He had an accomplice.
Did not seek publicity at first, and one would expect him to enjoy becoming an instant celebrity.	He enjoyed getting the publicity.	He would not have treated other police officers as his prime target.	The more damage done, the more he would look like a hero.
He had no past history of bomb making or radical statements.	He had problems in past jobs and needed a future job.	He would not have constructed an antipersonnel bomb.	The more damage done, the more he would look like a hero.
Most police officers do.	He had previous bomb training.	He had no reason to detonate the bomb early, before 30 minutes.	It went off accidentally.
Many people could have made the bomb.	The bomb was crude.	There were no witnesses or forensics linking him to the attack.	He took care to leave no fingerprints, assuming he would be a suspect.

hard to explain if Jewell's primary motive was just to keep himself employed.

Analytic Value Added: **Based upon your assessment of the Pros and Cons, can you make a strong case that Richard Jewell planted the bomb in Centennial Park?** The analysis generated by using the Pros-Cons-Faults-and-Fixes technique argues that the case against Jewell is highly circumstantial and that Jewell should not be treated as a prime—and particularly not as the only—target of the investigation. At this stage of the investigation, however, it also would appear imprudent to remove him from the list of possible suspects until further avenues of investigation are pursued. Key avenues for additional investigation would include these:

- Did the video surveillance cameras show anyone placing the knapsack under the bench?
- Did the surveillance cameras show any suspicious person or persons appearing to surveil the site in the days before the bombing?
- What actual experience did Jewell have in bomb making?
- Is there any forensic evidence in Jewell's car, on his clothes, or in his apartment indicating that he was in possession of bomb-making materials?
- Can we determine if Jewell was in Centennial Park when the phone call was made from the Days Inn?
- Is there any evidence of Jewell making radical statements justifying the use of violence or threatening violent acts?
- Did the 911 call fit a pattern of any previous bomb threats; did it stand out from the crowd of daily threats received by the police?

TECHNIQUE 3: MULTIPLE HYPOTHESIS GENERATION: MULTIPLE HYPOTHESES GENERATOR™

Multiple Hypothesis Generation is part of any rigorous analytic process because it helps the analyst avoid common pitfalls such as coming to premature closure or being overly influenced by first impressions. Instead, it helps the analyst think broadly and creatively about a range of possibilities. The goal is to develop an exhaustive list of hypotheses that can be scrutinized and tested over time against existing evidence and new data that may become available in the future.

The Multiple Hypotheses Generator™ is one of several tools that can be used to broaden the spectrum of plausible hypotheses. It is particularly helpful when there is a reigning lead hypothesis—in this case, the lead hypothesis that Richard Jewell planted the bomb in Centennial Park as part of a scheme to make himself a hero and obtain a position in law enforcement after the Olympic Games concluded.

The most important aspect of the tool is the discussion it generates among analysts about the range of plausible

Table 10.8 ▶ Atlanta Olympics Bombing Multiple Hypotheses Generator™: Brainstormed Alternatives Example

Lead Hypothesis: Richard Jewell planted the bomb to make himself a hero and help obtain a job.

Components	Lead Hypothesis	Alternatives		
Who?	Richard Jewell	International terrorists	Domestic violent extremists	Disgruntled contractors
What?	Antipersonnel bomb			
When?	27 July 1996			
Why?	To get a job	To inflict harm	To promote a political agenda	To protest losing a job
Where?	Centennial Park			
How?	Prepositioned explosive			

hypotheses, especially about the credibility score for each permutation. It is important to remember that the credibility score is meant to illuminate new, credible hypotheses for further examination. And while the process does encourage analysts to focus on the hypotheses with higher credibility scores, hypotheses with low credibility scores should not be entirely discarded because new evidence may emerge that changes their status.

Task 3.

Use the Multiple Hypotheses Generator™ to create and assess alternative hypotheses for the bombing in Centennial Park (see Table 10.8). Contact Globalytica, LLC at THINKSuite@globalytica.com or go to http://www.globalytica.com to obtain access to the Multiple Hypotheses Generator™ software if it is not available on your system.

Step 1: Identify the lead hypothesis and its component parts using Who? What? How? When? Where? and Why? using Table 10.4 in the book.

Richard Jewell placed the bomb under a bench in Centennial Park, alerted authorities to the bomb, and helped clear the area before the bomb exploded because he thought people would never know he placed the bomb and would consider him a hero for saving so many lives. With his reputation so enhanced, it would be easier for him to get a fulltime job as a police officer.

Steps 2 & 3: Identify plausible alternatives for each key component and strive to keep them mutually exclusive. Discard any "given" factors.

The "given" factors here include What (antipersonnel bomb), Where (Centennial Park), When (at 0120 on 27 July 1996), and How (prepositioned explosive); these will be the same for all hypotheses. Brainstorm possible alternatives for each of the remaining components, which in this case are Who and Why. Consolidate the lists into alternatives that are as mutually exclusive as possible. For example, al-Qaeda would have different motives than a radical domestic extremist group.

Step 4: Generate a list of possible permutations.

Step 5: Discard any permutations that simply make no sense.

Step 6: Evaluate the credibility of the remaining hypotheses on a scale of 1 to 5, where 1 is low credibility and 5 is high credibility.

The three hypotheses rated 0 in Table 10.9 can be discarded because they make little sense. For example, it makes no sense that terrorists would plant bombs to protest being laid off.

Step 7: Re-sort the remaining hypotheses, listing them from most to least credible, as shown in Table 10.10.

Step 8: Restate the permutations as hypotheses.

The permutations above are stated as hypotheses.

Step 9: Select from the top of the list those alternative hypotheses most deserving of attention and note why these hypotheses are most interesting (see Table 10.11).

The four most plausible hypotheses with a credibility score of 3 or higher are these:

- Richard Jewell planted the bomb to make himself a hero and obtain a job.
- International terrorists planted the bomb to inflict harm on America.

Table 10.9 ▶ Atlanta Olympics Bombing Multiple Hypotheses Generator™: Permutations and Credibility Scoring Example

Who?	Why?	Permutations	Credibility Score
International Terrorists	To inflict harm	International terrorists planted the bomb to inflict harm.	4
	To promote a political agenda	International terrorists planted the bomb to promote a political agenda.	1
	To protest losing a job	International terrorists planted the bomb to protest losing a job.	0
Domestic Violent Extremists	To inflict harm	Domestic violent extremists planted the bomb to inflict harm.	2
	To promote a political agenda	Domestic violent extremists planted the bomb to promote a political agenda.	4
	To protest losing a job	Domestic violent extremists planted the bomb to protest losing a job.	0
Disgruntled Workers	To inflict harm	Disgruntled workers planted the bomb to inflict harm.	1
	To promote a political agenda	Disgruntled workers planted the bomb to promote a political agenda.	0
	To protest losing a job	Disgruntled workers planted the bomb to protest losing a job.	3

Table 10.10 ▶ Atlanta Olympics Bombing Multiple Hypotheses Generator™: Sorted and Scored Hypotheses Example

Lead Hypothesis and Permutations	Credibility
Richard Jewell planted the bomb to make himself a hero and obtain a job.	4
International terrorists planted the bomb to inflict harm.	4
Domestic violent extremists planted the bomb to promote a political agenda.	4
Disgruntled workers planted the bomb to protest losing a job.	3
Domestic violent extremists planted the bomb to inflict harm.	2
International terrorists planted the bomb to promote a political agenda.	1
Disgruntled workers planted the bomb to inflict harm.	1

- Domestic violent extremists planted the bomb to promote a political agenda.
- Disgruntled workers planted the bomb to protest losing a job.

If none of these top four hypotheses generates serious investigative leads, then less highly rated hypotheses should receive increased attention.

It is possible that "disgruntled workers" might have planted a bomb out of a general sense of anger over losing their jobs but unlikely that they would target their anger at people attending the Olympics. A more likely target for them would be the nearby AT&T facility. International terrorists generally have not used terrorism to promote someone else's domestic political agenda, but it is possible they would collaborate in attacking the Olympic Games because it is an appropriate iconic target.

While the credibility score is subjective in nature, it should reflect reasoning that can be used to weed out nonsensical or highly unlikely hypotheses. The unused hypotheses should not be discarded. They should be reserved, and the list should be referred to and reconsidered as new information becomes available.

Analytic Value Added: Which hypotheses should be explored further? Use of the Multiple Hypotheses Generator™ flagged several new hypotheses that appear at least as credible as the lead hypothesis. Given the recent destruction of TWA 800, it would be imprudent not to consider international terrorists as a possible perpetrator. Domestic violent extremists might possess even stronger motives and capabilities to conduct such a bombing. The disgruntled workers hypothesis is probably less likely given the type of bomb used and its location, but it should not be dismissed at the onset of the investigation.

What motives should be considered, and why? Some of the more likely motives to emerge from the exercise would

Table 10.11 ▶ Atlanta Olympics Bombing Multiple Hypotheses Generator™: Hypotheses for Further Exploration Example

Hypotheses for Further Exploration	Reasoning
Richard Jewell planted the bomb to make himself a hero and obtain a job.	Jewell's past employment history makes him a candidate for a "wannabe" attack.
International terrorists planted the bomb to inflict harm.	International terrorists had struck several times at America, and the Olympics would be an iconic target.
Domestic violent extremists planted the bomb to promote a political agenda.	White supremacists, for example, could be protesting the multiethnic character of the Olympics, or anarchists could be targeting the Olympics to send out their nihilist message.
Disgruntled workers planted the bomb to protest losing a job.	Security guards who had recently been laid off were angry about losing their jobs.

be that the bomber has a personal agenda (to look like a hero); has an ideological agenda (to make a political statement or to promote an extremist cause such as white supremacy, the primacy of sovereign rights, anti-abortion, or anti-internationalism); or wants to do harm against people or institutions (perpetrators could range from local anarchists to al-Qaeda).

Which hypotheses from the original list were set aside, and why? It is up to the analyst to decide how many and which hypotheses should be considered for further exploration. A general rule of thumb is that more than five hypotheses become cumbersome and signal possible problems with mutual exclusivity. In such cases, analysts should be encouraged to aggregate hypotheses when taking a first look at the available evidence. Also, analysts should be encouraged initially to include hypotheses in the original list for which there is little or no evidence in the hope that new information might be obtained later that would support an initially outlier hypothesis. Hypotheses that are not based on observations, logic, or supportable assumptions, however, should not constitute a lead hypothesis. Analysts should state explicitly why certain hypotheses do not make the final list and record what new information could change that status in the future.

CONCLUSION

Two days after the bombing, President Bill Clinton told the American public that the Games should carry on as planned to show that the United States would not be cowed by acts of terrorism. He said: "An act of terrorism like this is clearly directed at the spirit of our own democracy. We must not let these attacks stop us from going forward. We cannot let terror win. That is not the American way."[1]

On 26 October 1996, Jewell was informed that he no longer was a target of the Atlanta Olympics bomb investigation. An internal investigation was launched inside the FBI focusing on whether Jewell's status as a prime suspect had been leaked to the media, but ultimately the Bureau never identified or disciplined anyone for the alleged leak.[2]

Following his ordeal, Jewell filed slander and libel lawsuits against several media organizations.[3] NBC, CNN, and the *New York Post* all settled their cases with Jewell for undisclosed amounts. Piedmont College, the school where Jewell was once employed, also settled for an undisclosed amount. Several school employees, including Cleere, had said unfavorable things about Jewell when they were interviewed by the FBI.

Months later, Jewell's attorney, Lin Wood, said that the role the media played in his client's status as a suspect was crucial. "We know," Wood said, "that the FBI was interested in Richard, but had really not decided whether Richard Jewell was a possible suspect or a potentially valuable witness. But before they could execute their plan, the banner headline gets published, and now all of a sudden, the FBI's got to come to grips with Richard Jewell in a public investigation, and that changed, I think, the whole approach that the FBI took."[4]

Jewell died on 29 August 2007 from natural causes at the age of 44. He was suffering from severe heart disease, kidney disease, and diabetes.[5]

THE HUNT FOR ERIC RUDOLPH

Over a two-year period after the bombing, special agents on the Southeast Bomb Task Force interviewed thousands of witnesses and traced nearly every component of the bomb. The task force was comprised of the FBI; Bureau of Alcohol, Tobacco, and Firearms (ATF); Georgia Bureau of Investigation; Alabama Bureau of Investigation; Birmingham Police Department; and prosecutors from the Justice Department. In addition, many local and state law enforcement units supported the task force.[6]

On 14 October 1998, federal authorities charged Eric Rudolph with conducting the fatal bombing at Atlanta's Centennial Park on 27 July 1996. Rudolph became a serious target of investigation in part because a Tennessee couple identified him as the man to whom they sold the smokeless powder believed to have been used in the Atlanta bomb device.[7]

Federal authorities also charged Rudolph with a double bombing at a health clinic in the Sandy Springs Professional Building in North Atlanta on 16 January 1977 and with the bombing of a gay night club, the Otherside Lounge, in Atlanta on 21 February 1997.[8] In the Sandy Springs bombing, the first bomb caused significant damage at the back of the building. The second bomb was designed to "kill and maim rescuers, paramedics, firefighters, and police officers who rushed to the scene to help," according to the Director of the ATF.[9] A second bomb was also found at the scene of the Otherside Lounge bombing, but the area was cleared before it exploded.

In addition, Rudolph was charged with the bombing at the New Woman All Woman Health Care Clinic in Birmingham, Alabama, on 29 January 1998, which killed Birmingham police officer Robert Sanderson and severely injured the clinic's head nurse, Emily Lyons. In announcing the charges against Rudolph, the government said it would pay a reward of $500,000 for information leading to a conviction of Rudolph and a reward of up to $1,000,000 for information leading to Rudolph's arrest.[10]

Rudolph became one of America's top ten most wanted fugitives from justice.[11] A sizeable law enforcement contingent, supported by infrared-equipped helicopters and tracking dogs, was dispatched to comb the 517,000-acre Nantahala Forest in western North Carolina to look for any sign of Rudolph.[12,13]

After more than five years on the run, Rudolph was captured in May 2003 when police spotted him near a trash bin in Murphy, North Carolina, apparently scavenging for food.[14] He was brought to trial in July 2004 and charged with the bombings of the health clinic and the Otherside Lounge in Atlanta, the bombing of the abortion clinic in Alabama, and the Centennial Park bombing.[15] Rudolph told federal investigators that his motive for planting the bomb in Centennial Park was to bring down the Olympic Games and embarrass the US government for legalizing abortion.[16]

In April 2005, Rudolph admitted to the crimes and, as part of a plea bargain, was spared the death penalty, receiving four consecutive life sentences without parole.[17] Deborah Rudolph, Rudolph's sister-in-law, said her brother-in-law accepted the government's offer of life without parole in exchange for admitting guilt in order to "protect his family from further scrutiny."[18] Rudolph characterized his decision as "purely a tactical choice," leaving open the question as to whether his confession for having conducted all four bombings was legitimate.[19]

KEY TAKEAWAYS

- When under severe pressure to find a culprit or generate an analytic conclusion quickly, an alarm should go off telling you that these are the circumstances where the use of structured analytic techniques is most justified.
- The use of techniques like the Key Assumptions Check or Pros-Cons-Faults-and-Fixes only take a few hours but can save investigators days, if not weeks, of energy they would otherwise waste tracking down low-priority leads or working from assumptions that upon close inspection prove invalid.
- Considering multiple credible hypotheses (or suspects) at the start of an investigation often proves much more efficient and less time-consuming overall than conducting the investigation in a serial fashion by first going after a prime suspect, and then a second suspect if the first does not pan out, and then a third suspect, etc. Considering multiple suspects also helps focus attention on the most diagnostic evidence.

INSTRUCTOR'S READING LIST

Federal Bureau of Investigation, Counterterrorism Division, Counterterrorism Threat Assessment and Warning Unit, National Security Division. "Terrorism in the United States: 1996." http://www.fbi.gov/stats-services/publications/terror_96.pdf.

Ostrow, Ron. "Richard Jewell and the Olympic Bombing: Case Study." Pew Research Center's Project for Excellence in Journalism. February 15, 2003. http://www.journalism.org/node/1791.

NOTES

1. BBC, "1996: Bomb Rocks Atlanta Olympics," http://news.bbc.co.uk/onthisday/hi/dates/stories/july/27/newsid_3920000/3920865.stm.
2. Iver Peterson, "Head of FBI Says It Can't Trace Disclosure in Olympic Bombing Case," *New York Times,* December 20, 1996, http://www.nytimes.com/1996/12/20/us/head-of-fbi-says-it-canttrace-disclosure-in-olympic-bomb-case.html.
3. Harry R. Weber, "Former Olympic Park Guard Jewell Dies," *Washington Post,* August 30, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/08/30/AR2007083000324.html.
4. David Kohn, "Falsely Accused," 60 Minutes II, CBS Worldwide, June 26, 2002, http://www.cbsnews.com/stories/2002/01/02/60II/main322892.shtml.
5. Kevin Sack, "Richard Jewell, 44, Hero of Atlanta Attack Dies," *New York Times,* August 30, 2007, http://www.nytimes.com/2007/08/30/us/30jewell.html?n=Top/Reference/Times%20Topics/Subjects/O/Olympic%20Games.
6. Department of Justice, "Eric Rudolph Charged in Centennial Olympic Park Bombing" [press release], October 14, 1998, http://www.fas.org/irp/news/1998/10/477crm.htm.
7. BBC, "1996: Bomb Rocks Atlanta Olympics."
8. Department of Justice, "Eric Rudolph Charged in Centennial Olympic Park Bombing."
9. Ibid.
10. Ibid.
11. "Key Dates in Hunt for Eric Rudolph," Fox News, June 2, 2003, http://www.foxnews.com/story/0,2933,88269,00.html.
12. "Search for Rudolph Continues 5 Years After Bombing," CNN, July 23, 2001, http://articles.cnn.com/2001–07–23/justice/rudolph.search_1_emily-lyons-eric-robert-rudolph-double bombing.
13. Paul Nowell, "Search for Bombing Suspect Resumes," *Washington Post*, July 12, 1999, http://www.washingtonpost.com/wp-srv/national/longterm/rudolph/rudolph.htm.
14. Associated Press, "Raw Data: Timeline in Eric Rudolph Case," Fox News, June 2, 2003, http://www.foxnews.com/story/0,2933,88269,00.html.
15. BBC, "1996: Bomb Rocks Atlanta Olympics."
16. Mike Lopresti, "A Decade Later, Atlanta Olympic Bombing Overshadowed," *USA Today,* July 23, 2006, http://www.usatoday.com/sports/columnist/lopresti/2006–07–23-lopresti-atl-10-years_x.htm.
17. BBC, "1996: Bomb Rocks Atlanta Olympics."
18. Henry Schuster, "Why Did Rudolph Do It?" CNN, April 15, 2005, http://www.cnn.com/2005/US/04/11/schuster.column/index.html.
19. Associated Press, "Eric Rudolph Gets Life Without Parole," Fox News, July 18, 2005, http://www.foxnews.com/story/0,2933,162790,00.html.

Table 11.1 ▶ Case Snapshot: The DC Sniper		
Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Key Assumptions Check	p. 209	Assessment of Cause and Effect
Multiple Hypotheses Generator™	p. 173	Hypothesis Generation and Testing
Classic Quadrant Crunching™	p. 122	Idea Generation

11 The DC Sniper
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

In a crisis, it is easy to allow the pace of breaking events to lead to the first, most obvious answers. This case highlights the importance of using a systematic process early in a project to avoid this temptation. The techniques help analysts to frame the issue effectively by challenging faulty mental models and generating a full array of possible explanations. The Key Assumptions Check does this by helping analysts explicate and challenge implicit assumptions about the sniper. The Multiple Hypotheses Generator™ and Classic Quadrant Crunching™ exercises are two prisms through which analysts can systematically develop and begin to assess a range of possible explanations. In this case, the Multiple Hypotheses Generator™ highlights the need to consider a broader range of suspects, and Classic Quadrant Crunching™ helps uncover new dimensions for consideration, many of which had direct bearing on the true outcome of the case.

TECHNIQUE 1: KEY ASSUMPTIONS CHECK

The Key Assumptions Check is a systematic effort to make explicit and question the assumptions that guide an analyst's interpretation of evidence and reasoning about any particular problem. Such assumptions are usually necessary and unavoidable as a means of filling gaps in the incomplete, ambiguous, and sometimes deceptive information with which the analyst must work. They are driven by the analyst's education, training, and experience, including the organizational context in which the analyst works. It can be difficult to identify assumptions, because many are sociocultural beliefs that are held unconsciously or so firmly that they are assumed to be truth and not subject to challenge. Nonetheless, identifying key assumptions and assessing the overall impact should conditions change are critical parts of a robust analytic process.

Task 1.

Conduct a Key Assumptions Check of the initial theory that the shooter most likely fits the profile of a classic serial killer—a lone, white male with some military experience.

Step 1: Gather a small group of individuals who are working the issue along with a few "outsiders." The primary analytic unit already is working from an established mental model, so the "outsiders" are needed to bring other perspectives.

In this instance, expert commentators interviewed on the various TV networks—and the public in general—played the role of "outsiders." As it turned out, the expert commentators' perspectives tracked closely with the FBI's regarding the most likely criteria, focusing on the theory of a serial killer. This tended to reinforce the theory of a lone, white male shooter when other options deserved more serious consideration.

Step 2: Ideally, participants should be asked to bring their lists of assumptions when they come to the meeting. If not, start the meeting with a silent brainstorming session. Ask each participant to write down several assumptions on 3 × 5 cards.

Step 3: Collect the cards and list the assumptions on a whiteboard for all to see. A simple template can be used, like the one shown in Table 11.2.

In the early days of the investigation, the lead hypothesis had four key components:

- **Lone**—Only one shooter was involved in the multiple shootings.
- **White**—Serial killers are almost always Caucasian.
- **Male**—Serial killers are almost always male.
- **Military experience**—The shooter must have had military experience in order to shoot so well and may have even been a sharpshooter.

Step 4: Elicit additional assumptions. Work from the prevailing analytic line back to the key arguments that support it. Use various devices to help prod participants' thinking. Ask the standard journalist questions: Who? What? How? When? Where? and Why? Phrases such as "will always," "will never," or "would have to be" suggest that an idea is not being challenged and perhaps should be. Phrases such as "based on" or "generally the case" usually suggest that a challengeable assumption is being made.

For the purposes of this case study, it works best to focus the conversation on the lone, white male theory. At the time, other explanations were considered, including the possibility that the shooter was a foreign terrorist; a domestic extremist, and possibly a white supremacist because several persons of color were killed; or a disgruntled employee of Michael's, Home Depot, or gas stations where the shootings took place.

Step 5: After identifying a full set of assumptions, critically examine each assumption. Ask:

- Why am I confident that this assumption is correct?
- In what circumstances might this assumption be untrue?
- Could this assumption have been true in the past but no longer be true today?
- How much confidence do I have that this assumption is valid?
- If this assumption turns out to be invalid, how much impact would it have on the analysis?

Step 6: Using Table 11.2, place each assumption in one of three categories:

- Basically supported
- Supported with some caveats
- Unsupported or questionable—the "key uncertainties"

Table 11.6 ▶ Key Assumptions Check: DC Sniper as a Serial Killer

Key Assumption	Commentary	Supported	With Caveats	Unsupported
1. Lone	Empirical studies show that 80 percent of serial killers operate alone and only 12 percent with partners. This is a fairly good assumption for planning purposes, but analysts should be alert to the possibility of a partner being involved.		✓	
2. White	Empirical studies show that about 80 percent of all serial killers are Caucasians. If we were to assume that the shooter is a Caucasian, we would be ruling out 20 percent of the potential targets—an even bigger mistake.		✓	
3. Male	Empirical studies show that about 85 percent of all serial killers are male. Again, this is a good operating assumption, but we should be alert to any indications this case could prove to be an exception.		✓	
4. Military experience	The weapon used was a high-caliber Bushmaster rifle. Most people require only a few hours of training to learn how to use a Bushmaster with some accuracy, particularly if it has a scope and a tripod or something else to stabilize the shooting platform.			✓

A critical review of the assumptions would place three assumptions in the With Caveats category and one assumption in the Unsupported category, as shown in Table 11.6.

Step 7: Refine the list, deleting those assumptions that do not hold up to scrutiny and adding new assumptions that emerge from the discussion.

- The assumption that a serial killer would be operating alone is rated as "With Caveats," given that 12 percent of serial killers have partners.[1] Given the spectacular nature of this case and how little is known about the shootings, it would be premature to discount the possibility of the killer operating with a confederate. In fact, the students might point out that one characteristic of the case—that the shootings occurred with neither the shooter nor anyone departing the scene observed—would argue that the shooter was using a mobile shooting platform and would need a driver to ensure a quick getaway.
- Assuming the shooter must be a Caucasian would be a major mistake, as this would rule out 20 percent of all possible suspects despite no case evidence suggesting the shooter is a Caucasian.[2] In fact, one of the police reports relating to the first shooting into a Michael's craft store noted that two black males were seen departing the parking lot in a suspicious manner.
- Knowing that 85 percent of all serial killers are males suggests that this would be a solid assumption for mounting an investigation.[3] However, given the spectacular nature of the crimes, the urgency of the problem, and the lack of evidence at this stage of the investigation, it would be make more sense not to rule out any options and list this assumption as With Caveats.
- The assumption that the shooter must have military experience is reasonable but certainly not conclusive. Most people could learn to shoot a Bushmaster with little training. More important, a discussion of this assumption should prompt a much more productive exploration of what is needed to shoot people with such accuracy. When asked this question, most students immediately respond by suggesting the value of having a scope on the rifle. Usually with a little more time they suggest a tripod or something that can be used to stabilize the rifle. Since the shooter has not been seen yet, this begs two questions: Where is the shooter shooting from? and How would he be able to stabilize the shooting platform? One answer is that he might be shooting from a van or some other vehicle with a built-in shooting platform.

Step 8: Consider whether key uncertainties should be converted into collection requirements or research topics.

Analytic Value Added: Did the FBI investigators inherit any key assumptions when they took over the case that had an impact on how effectively they pursued the case? What is the value of conducting a Key Assumptions Check at the beginning of a major investigation? What impact did key assumptions have on how the investigation was conducted? In this case, a Key Assumptions Check exercise, if conducted, would have reinforced Montgomery County Police Chief Moose's views that the investigation should not prematurely focus only on whites but should consider persons of all races as suspect. It might also have warned investigators not to give military experience undue weight in conducting the investigation. In addition, a Key Assumptions Check could have sparked a discussion of how the shooter was taking shots, what kinds of vehicles might be involved, and whether the perpetrator would need an accomplice. Lastly, it would have sensitized the investigators to several wild-card possibilities that the shooter could be a non-Caucasian, a female, or operating with a partner. Although historically the chances of these possibilities being true were remote, if evidence surfaced later in the investigation pointing to any of these three possibilities, it would have been helpful to have a "bin" to place that evidence in. In fact, from the outset of the case there was evidence, mostly in the form of eyewitness accounts, that black males were seen acting suspiciously in the vicinity of the crime, and about halfway through the investigation evidence began to surface that more than one shooter was involved.

TECHNIQUE 2: MULTIPLE HYPOTHESIS GENERATION: MULTIPLE HYPOTHESES GENERATOR™

The Multiple Hypotheses Generator™ is a useful tool for broadening the spectrum of plausible hypotheses. It is particularly useful when there is a reigning lead hypothesis—in this case, the FBI profile—and there are few facts to prove or disprove it. The most important aspect of the tool is the discussion it generates among analysts about the range of plausible hypotheses, especially about the relative credibility of each permutation. It is important to remember that the

credibility score is meant to illuminate new, credible hypotheses for further examination. And although the process encourages analysts to focus on the hypotheses with the highest credibility scores, hypotheses with low credibility scores should not be entirely discarded because new evidence could emerge that could make a hypothesis more credible.

Task 2.

Use the Multiple Hypotheses Generator™ (see Table 11.3) to create and assess alternative hypotheses. Contact Globalytica, LLC at THINKSuite@globalytica.com or go to http://www.globalytica.com to obtain access to the software if it is not available on your system.

Step 1: Identify the lead hypothesis and its component parts.

In this example, the Who, Why, and What have been explored. The lead hypothesis could best be articulated as follows: A white male is driving a white van and killing to extort money. The key components are "white male," "white van," and "killing to extort money." Since it is a fact that shootings are happening and that the ballistic tests have resulted in the identification of the type of weapon used, these aspects can be considered to be static and need not be included in the permutations.

Steps 2 & 3: Identify plausible alternatives for each key component and strive to keep them mutually exclusive. Discard any "given" factors such as the *How* (shooting) that will be the same for all hypotheses. Table 11.7 shows the results of a brainstorming session on alternatives.

The students are likely to suggest additional alternatives, but the two alternatives listed above have generally proven most effective in illustrating the technique. For example, other alternatives to "White Male" could be "Hispanic" or "Middle Easterner." Similarly, possible alternatives to "White Van" are "Public Transportation," "Motorcycle," or "Bicycle." Any of these could be substituted for "On Foot." The Why? question usually prompts a robust discussion, and almost any alternative is worthy of consideration, including "Hate Crime," "Corporate Grievance," "Gang Initiation," or "Political Protest." At the time, some cited "Hate Crime" as the motive because of the number of persons of color killed, maintaining that the shooting of whites was intended to disguise the shooters' true motive. Similarly, some analysts suggested that the killers were aggrieved employees of Michael's Arts & Crafts store, Home Depot, or gas stations because of the locations of the shootings.

Table 11.7 ▶ DC Sniper Multiple Hypotheses Generator™: Matrix of Alternative Hypotheses

Lead Hypothesis: A white male is driving a white van and killing to extort money.

Components	Lead Hypothesis	Alternative/Brainstormed	
Who?	White Male	Black Male	White Female
What?	White Van	Sedan	On Foot
Why?	To Extort Money	Seek Fame	Cause Terror

Steps 4, 5, & 6: Generate a list of possible permutations, discard any permutations that simply make no sense, and evaluate the credibility of the remaining hypotheses on a scale of 1 to 5, where 1 is low credibility and 5 is high credibility.

Table 11.8 contains the list of all the permutations along with their respective credibility score. All permutations made sense, and therefore none has been discarded.

When evaluating the credibility of the hypotheses, it is important to consider each element separately and work across the permutation table. The discussion points below describe this process and list the underlying facts and assumptions that contributed to the credibility scores in the figure.

- All permutations with "On Foot" received a credibility score of 1 because it is highly unlikely that the shooter could successfully travel by foot with a concealed rifle of the caliber used in the shootings and not be detected.
- Permutations for a "White Female" sniper received a credibility score of 2 because snipers are historically less likely to be female. Nonetheless, the credibility score is higher than the scores above because females have engaged in terrorist attacks, and we cannot rule out hypotheses on the absence of evidence alone.
- Of the remaining permutations for "White Male," it seems equally plausible that the sniper could be working from a "White Van" or "Sedan," and therefore the scores are the same for these two elements.
- The sniper activities were very successful in instilling terror, so this alternative received a credibility score of 5.

Table 11.8 ▶ DC Sniper Multiple Hypotheses Generator™: Permutation Tree

Who?	What?	Why?	Permutations	Credibility Score
White Male	White Van	Extort Money	A white male is killing to extort money and is driving a white van.	4
		Terrorize	A white male is killing to cause terror and is driving a white van.	5
		Seek Fame	A white male is killing to seek fame and is driving a white van.	3
	Sedan	Extort Money	A white male is killing to extort money and is driving a sedan.	4
		Terrorize	A white male is killing to cause terror and is driving a sedan.	5
		Seek Fame	A white male is killing to seek fame and is driving a sedan.	3
	On Foot	Extort Money	A white male is killing to extort money and is on foot.	1
		Terrorize	A white male is killing to cause terror and is on foot.	1
		Seek Fame	A white male is killing to seek fame and is on foot.	1
White Female	White Van	Extort Money	A white female is killing to extort money and is driving a white van.	2
		Terrorize	A white female is killing to cause terror and is driving a white van.	2
		Seek Fame	A white female is killing to seek fame and is driving a white van.	2
	Sedan	Money	A white female is killing to extort money and is driving a sedan.	2
		Terrorize	A white female is killing to cause terror and is driving a sedan.	2
		Seek Fame	A white female is killing to seek fame and is driving a sedan.	2
	On Foot	Money	A white female is killing to extort money and is on foot.	1
		Terrorize	A white female is killing to cause terror and is on foot.	1
		Seek Fame	A white female is killing to seek fame and is on foot.	1
Black Male	White Van	Extort Money	A black male is killing to extort money and is driving a white van.	4
		Terrorize	A black male is killing to cause terror and is driving a white van.	5
		Seek Fame	A black male is killing to seek fame and is driving a white van.	3
	Sedan	Extort Money	A black male is killing to extort money and is driving a sedan.	4
		Terrorize	A black male is killing to cause terror and is driving a sedan.	5
		Seek Fame	A black male is killing to seek fame and is driving a sedan.	3
	On Foot	Extort Money	A black male is killing to extort money and is on foot.	1
		Terrorize	A black male is killing to cause terror and is on foot.	1
		Seek Fame	A black male is killing to seek fame and is on foot.	1

- Given the difficulty the sniper had in making arrangements to extort money from the authorities, "Extort Money" received a slightly lower score of 4.
- It is possible the sniper is acting out of a desire to seek fame, but there is less evidence in the case to support this alternative, so "Seek Fame" received a credibility score of 3.
- For the remaining "Black" permutations, as with "White," there is no variation in credibility score between "White Van" and "Sedan." Also like "White," "Seek Fame" received a score of 3.
- For the "White" permutations, "Extort Money" and "Terrorize" received scores of 4 and 5 to reflect the fact that historically, similar attacks have been committed by white males. Although this case may challenge this historical precedent, there is not yet a strong reason to lower this score.

Step 7: Re-sort the remaining hypotheses from most to least credible, as shown in Table 11.9.

Table 11.9 ▶ DC Sniper Hypotheses Re-sorted by Credibility

Permutations	Credibility Score
A white male is killing to cause terror and is driving a white van.	5
A white male is killing to cause terror and is driving a sedan.	5
A black male is killing to cause terror and is driving a white van.	5
A black male is killing to cause terror and is driving a sedan.	5
A white male is killing to extort money and is driving a white van.	4
A white male is killing to extort money and is driving a sedan.	4
A black male is killing to extort money and is driving a white van.	4
A black male is killing to extort money and is driving a sedan.	4
A white male is killing to seek fame and is driving a white van.	3
A white male is killing to seek fame and is driving a sedan.	3
A black male is killing to seek fame and is driving a white van.	3
A black male is killing to seek fame and is driving a sedan.	3
A white female is killing to extort money and is driving a white van.	2
A white female is killing to cause terror and is driving a white van.	2
A white female is killing to seek fame and is driving a white van.	2
A white female is killing to extort money and is driving a sedan.	2
A white female is killing to cause terror and is driving a sedan.	2
A white female is killing to seek fame and is driving a sedan.	2
A white male is killing to extort money and is on foot.	1
A white male is killing to cause terror and is on foot.	1
A white male is killing to seek fame and is on foot.	1
A white female is killing to extort money and is on foot.	1
A white female is killing to cause terror and is on foot.	1
A white female is killing to seek fame and is on foot.	1
A black male is killing to extort money and is on foot.	1
A black male is killing to cause terror and is on foot.	1
A black male is killing to seek fame and is on foot.	1

Step 8: Restate the permutations as hypotheses.

The permutations above are stated as hypotheses.

Step 9: Select from the top of the list those alternative hypotheses most deserving of attention and note why these hypotheses are most interesting.

For this example, we have selected those permutations with a credibility score of 3 or higher as deserving the most attention based on the reasoning detailed in step 6 (see Table 11.10).

Analytic Value Added: In light of your findings, how should investigators in the DC Sniper case have used this information? What new suspects should they have pursued? When the permutations with a credibility score of 3 or higher are listed together, it quickly becomes apparent that the task force might need to consider a broader range of suspects. Credibility scores suggest that it is just as plausible for the sniper to be working from a white van as it is from a sedan. It also becomes apparent that the task force might consider looking for both black males and

Table 11.10 ▶ DC Sniper Multiple Hypotheses Generator™: Top Hypotheses

Permutations	Credibility Score
A white male is killing to cause terror and is driving a white van.	5
A white male is killing to cause terror and is driving a sedan.	5
A black male is killing to cause terror and is driving a white van.	5
A black male is killing to cause terror and is driving a sedan.	5
A white male is killing to extort money and is driving a white van.	4
A white male is killing to extort money and is driving a sedan.	4
A black male is killing to extort money and is driving a white van.	4
A black male is killing to extort money and is driving a sedan.	4
A white male is killing to seek fame and is driving a white van.	3
A white male is killing to seek fame and is driving a sedan.	3
A black male is killing to seek fame and is driving a white van.	3
A black male is killing to seek fame and is driving a sedan.	3

white males. The exact motive is less important than knowing the Who and What, but examining the potential reasons may assist investigators in how they approach the investigation and potential future communication with the sniper. Using the Multiple Hypotheses Generator™ allowed each aspect of the alternative hypotheses to be evaluated in a robust manner that explicitly detailed the facts and assumptions underlying each credibility score. These conversations are often enlightening and may not happen if the technique is not used.

TECHNIQUE 3: CLASSIC QUADRANT CRUNCHING™

Classic Quadrant Crunching™ combines the methodology of a Key Assumptions Check with Multiple Scenarios Generation to generate an array of alternative scenarios or stories. This process is particularly helpful in the DC Sniper case because of embedded assumptions in the FBI profile, witness reports of white vans, and the contents of the demand note. This technique allows the user to look at and challenge those key assumptions. When combined with the Multiple Hypotheses Generator™, this technique provides a strong basis for developing and considering alternative explanations and scenarios.

Task 3.

Use Classic Quadrant Crunching™ to challenge the key assumptions in the case that is listed below.

Step 1 & 2: State your lead hypothesis or key assumption and break it down into its component parts. For the purposes of this exercise: A lone white male is conducting the shootings from a white van to extort money.

The words "lone," "white," "white van," and "to extort money" are the component parts to be explored. Since it is a fact that shootings are happening and that the ballistic tests have identified the type of rifle, neither of these aspects is included.

Step 3: Identify contrary assumptions and two contrary dimensions in a template like that shown in Table 11.4.

Table 11.11 details the brainstormed contrary assumptions and two contrary dimensions.

The students are likely to suggest additional contrary dimensions, but the pairs listed in Table 11.11 are effective in illustrating the technique. For example, other possibilities in the Other Transportation Method category are "Public Transportation," "Motorcycle," or "Bicycle." Any of these could be substituted for "On Foot." Similarly, in the Multiple Attackers category, some might suggest "independent shooters," and in the Other Race category, some might suggest Middle Easterners. The Other Motivation category usually prompts a robust discussion, and almost any alternative is worthy of consideration, including "Hate Crime" and "Corporate Grievance." At the time, some cited "Hate Crime" as the motive because of the number of persons of color killed, maintaining that the shooting of whites was intended to disguise the shooters' true motive. Similarly, some analysts suggested that the killers were aggrieved employees of Michael's Arts and Crafts, Home Depot, or gas stations because of the locations of the shootings.

Step 4: Array combinations of these contrary assumptions in a set of 2 × 2 matrices.

From the contrary dimensions, 6 matrices are possible for a total of 24 cells, as shown in Table 11.12. For ease of discussion, each 2 × 2 matrix and quadrant have been given a letter and number identifier. For example, in the first matrix, A/B-1 refers to the quadrant with a team of black shooters.

Step 5: Generate scenarios for each quadrant.

For each cell in each matrix, generate one to three examples of how this scenario might happen. For example,

Table 11.11 ▶ DC Sniper Classic Quadrant Crunching™ Dimensions

Key Assumptions	Contrary Assumption	Contrary Dimensions	
A. Lone Attacker	Multiple Attackers	Team	Copycat Killers
B. White	Other Race	Black	Hispanic
C. White Van	Other Transportation Method	Sedan	On Foot
D. To Extort Money	Other Motivation	Seek Fame	Cause Terror

Table 11.12 ▶ DC Sniper Classic Quadrant Crunching™: 2 × 2 Matrices

A/B	Multiple Attackers/Race		
1	Team Black	3	Team Hispanic
2	Copycat Killers Black	4	Copycat Killers Hispanic
A/C	Multiple Attackers/Transport		
1	Team Sedan	3	Team On Foot
2	Copycat Killers Sedan	4	Copycat Killers On Foot
A/D	Multiple Attackers/Motivation		
1	Team Seek Fame	3	Team Cause Terror
2	Copycat Killers Seek Fame	4	Copycat Killers Cause Terror
B/C	Race/Transport		
1	Black Sedan	3	Black On Foot
2	Hispanic Sedan	4	Hispanic On Foot
B/D	Race/Motivation		
1	Black Seek Fame	3	Black Cause Terror
2	Hispanic Seek Fame	4	Hispanic Cause Terror
C/D	Transport/Motivation		
1	Sedan Seek Fame	3	Sedan Cause Terror
2	On Foot Seek Fame	4	On Foot Cause Terror

Quadrant A/B-1 is a team of black snipers that is conducting attacks in multiple locations across the metropolitan Washington, D.C., area. The snipers formed a team sometime over the past year and set their well-practiced plan in motion after several months of planning and training. The circumstances surrounding the formulation of their group and the exact number of members in the cell are unknown. As a result, if this team is quite small, they could be conducting the attacks one at a time. If the team is larger and dispersed, they could be conducting coordinated attacks at preappointed times.

In some cases, such a scenario might already have been imagined. In other quadrants, it will be difficult to come up with a credible scenario. But several of the quadrants will usually stretch the analysts' thinking, forcing them to think about the dynamic in new and different ways.

Step 6: Select those scenarios (cells) deserving the most attention.

Review all the scenarios generated in Step 5 and select those most deserving of attention based on a pre-established set of criteria. In this example, possible criteria might include those scenarios that would be the hardest to detect or prevent. This would include those scenarios in which a team operates on foot and would have difficulty exiting the scene of the crime undetected. Similarly, copycat killers might have difficulty making arrangements to extort for money.

Another way to narrow the list of cells in this case is to remove those cells that are less likely either because of known facts in the case or due to strong historical precedent. As a result, the following scenarios were excluded:

- Cells with "Copycat Killers" were given low priority because ballistic tests indicated only one type of rifle, a Bushmaster .223, was used and it seems highly improbable that imitative snipers would be using the same weapon.
- "On Foot" cells have been excluded because it seems highly improbable that the shooter, carrying a rifle, would go unnoticed at the scene of the crime. While some rifles disassemble quickly, it would be easy to further refute this by examining those weapons capable of firing the .223 round to determine if they are capable of easily being disassembled. In addition, a review of public transportation available near the shooting sites could further discount such a scenario.

This process results in dropping 11 of the 24 scenarios from our list of priority combinations. In this case, all the scenarios could be defined as nightmare scenarios because they all have an unknown probability but high impact: the metropolitan Washington, D.C., area is being terrorized by a sniper who is killing at a high rate. The main elements that are shared by all the remaining scenarios and that appear most deserving of further attention are these:

- "Team" cells could explain how the shooter gets away so quickly. One person shoots, and one acts as the driver/lookout.

- "Sedan" cells could explain why the dragnets that have been looking for a white van have failed to catch the sniper.
- Cells with either race option seem equally probable and are both worth considering in addition to the lead hypothesis, which is white.
- Cells with "Cause Terror" seem realistic since the attacks were causing severe and widespread fear.

It is important to remember that although we have identified some cells as deserving of the most attention, we do not delete or discard the other cells. New information could be discovered that would increase the plausibility of those cells.

Step 7: Develop indicators for the selected scenarios.

The goal of developing indicators for each scenario is to help investigators look for and be aware of a broad range of scenarios and indications that one or another scenario may be emerging. For example, indicators of scenario B/C-1, a black sniper using a sedan, would encourage investigators not to disregard additional reports of sedans leaving the area and to review previous reporting and contact witnesses who previously reported the presence of a sedan. Reports that the shooter had a Hispanic accent when talking on the telephone provide strong justification for considering Hispanics in addition to whites. The discussion of matrix B/D that focuses on race and motivation, however, should surface the fact that blacks, whites, and Hispanics can have a Hispanic accent, as is often the case in the Caribbean. Without this analytic process forcing a critical examination of all credible alternatives, authorities might prematurely—and incorrectly—focus their investigation on Hispanics and ignore other credible suspects.

Analytic Value Added: Which alternative scenarios should investigators have pursued, and why? By critically examining each assumption and how a contrary assumption might play out, analysts can better assess their level of confidence in their predictions, the strength of their lead hypothesis, and the likelihood of their lead scenario. In the DC Sniper case, the use of this technique revealed some interesting possibilities that may not have otherwise been considered. This is of particular note because some of the cells in gray are what actually was happening—specifically A/B-1, A/C-1, and B/C-1. The hypotheses that contained "Black," "Team," and "Sedan" were accurate. While the motive of the snipers remains a bit confused to this day, and money certainly was a factor, terror and fame also played a role. In fact, the only erroneous cells were those with "On Foot," "Copycat Killers," and "Hispanic." Out of 24 cells, 13 were identified as deserving serious attention, and of those 13, 9 contained accurate elements.

CONCLUSION

The terror finally ended on 24 October 2002. One black man, John Allen Muhammad, formerly in the US Army, and one black teen, John Lee Malvo, of Jamaican decent, were caught sleeping at a rest stop off I-70 in Maryland when the authorities arrested them.[4] Malvo's Jamaican accent had been misinterpreted as Hispanic. The vehicle they were sleeping in was a blue 1990 Chevy Caprice.[5] The snipers had modified the vehicle by removing the metal divider between the backseat and the trunk and by making a hole above the license plate so that Muhammad and Malvo could fire from inside the car.[6] Authorities also found in the car a Bushmaster rifle, considered to be easy to use,[7] along with a scope and tripod.[8]

The note left at the Ponderosa did in fact use a plural pronoun, "we," and a note left after the Johnson shooting used "us."[9] Muhammad and Malvo had also attempted to contact the police multiple times. In fact, it was during one of their attempts to contact the police that they gave away crucial information. The snipers referred to a crime in Montgomery, Alabama, that would prove invaluable in identifying the suspects.[10] At that crime, fingerprint and ballistics had been obtained that pointed the task force directly at Malvo and, through him, to Muhammad.[11] In addition, a former army buddy of Muhammad's called the police on 17 October and was interviewed on 22 October.

The exact motive for the killing spree remains unclear. Malvo reportedly gave at least two reasons. The first was that "whites had tried to hurt Louis Farrakhan."[12] When asked directly if money was the reason for the killings, Malvo indicated yes and said that Montgomery County was chosen "because that's where the 'rich people' lived."[13] At Muhammad's trial, the motive argued by the prosecutor was revenge over a lost custody battle with Muhammad's wife.[14] Specifically, Malvo testified that the plan was to create havoc to cover for Mr. Muhammad's plans to kidnap his three children.

> The longer-term goal . . . was to extort law enforcement to stop the killing, after which Mr. Muhammad would take the money and move to Canada with Mr. Malvo and the

> three children. There . . . Mr. Muhammad planned to create a training ground for 140 young homeless men whom he would send out to wreak similar havoc and to "shut things down" in cities across the United States.[15]

At Malvo's trial, the financial motive was further expanded on by a claim that Muhammad intended to create "a black utopia in Canada populated by 70 boys and 70 girls who had been unexposed to racism."[16]

On 4 May 2004, Muhammad was sentenced to death in Virginia, and on 1 June 2006, he was sentenced to six life terms without parole in Maryland.[17,18] On 7 August 2009, the death sentence was upheld by the Fourth US Circuit Court of Appeals, and he was executed in Virginia on 10 November 2009.[19,20]

On 19 December 2003, Malvo was sentenced in Virginia to life imprisonment without the possibility of parole, and on 8 November 2006, he received six more years in Maryland in addition to the life sentence, all to be served consecutively.[21,22]

KEY TAKEAWAYS

- Decision making based on faulty assumptions can impede an investigation. Always explicitly identify and assess the effect implicit assumptions may have on an investigation.
- The tendency to "plunge in" should always be tempered by a process designed to identify all evidence and evaluate all possible explanations.
- Failure to consider alternative explanations from the start can slow an investigation and let the real killer avoid prosecution.
- Employing a more systematic process at the start of the investigation to better frame the issue helps analysts identify unproductive blind alleys early on and avoid them.

INSTRUCTOR'S READING LIST

Horwitz, Sari, and Michael E. Ruane. *Sniper: Inside the Hunt for the Killers Who Terrorized the Nation*. New York: Random House, 2003.

NOTES

1. James Alan Fox and Jack Levin, "An Anatomy of Serial Murder," chap. 3 in *Extreme Killing: Understanding Serial and Mass Murder* (London: Sage, 2005), 38. Available at http://www.sagepub.com/upm-data/5396_Fox_Final_Pages_Chapter_3.pdf.
2. Ibid.
3. Ibid.
4. "A Byte Out of History: The Beltway Snipers, Part 1," FBI Online, October 22, 2007, http://www.fbi.gov/news/stories/2007/october/snipers_102207.
5. "Closing the Net: How They Cracked the Case," CNN, October 25, 2002, http://edition.cnn.com/2002/US/South/10/24/sniper.case.cracked/index.html.
6. "A Byte Out of History: The Beltway Snipers, Part 1," FBI Online.
7. "Bushmaster .223: Accurate, Inexpensive," CNN, October 24, 2002, http://articles.cnn.com/2002–10–24/us/sniper.bushmaster.rifle_1bushmaster-semi-automatic-rifle-weapon.
8. "Closing the Net: How They Cracked the Case," CNN.
9. Sari Horwitz and Michael E. Ruane, *Sniper: Inside the Hunt for the Killers Who Terrorized the Nation* (New York: Random House, 2003), 170, 188.
10. Ibid., 163–65.
11. "A Byte Out of History: The Beltway Snipers, Part 1," FBI Online.
12. Horwitz and Ruane, *Sniper: Inside the Hunt for the Killers Who Terrorized the Nation*, 234.
13. Ibid., 235.
14. "Jury Convicts Malvo of Sniper Murder," CNN, December 19, 2003, http://articles.cnn.com/2003–12–18/justice/sprj.dcsp.malvo.trial_1_jury-convicts-malvo-lee-boyd-malvo-michael-arif.
15. "Washington-Area Sniper Convicted of 6 More Killings," *New York Times,* May 31, 2006, http://www.nytimes.com/2006/05/31/us/31sniper.html.
16. "Jury Convicts Malvo of Sniper Murder," CNN.
17. "Sniper Muhammad Sentenced to Death," CNN, May 5, 2004, http://edition.cnn.com/2004/LAW/03/09/sniper/index.html.
18. Associated Press, "D.C.-Area Sniper Gets 6 Life Terms in Maryland," MSNBC Online, June 1, 2006, http://www.msnbc.msn.com/id/13082594/ns/us_news-crime_and_courts/t/dc-area-sniper-gets-life-terms-maryland.
19. Associated Press, "Appellate Court Upholds D.C. Sniper Conviction," *Richmond* (Virginia) *Times-Dispatch,* August 8, 2009, http://www2.timesdispatch.com/news/2009/aug/08/snip08_20090807–215605-ar-34831.
20. Josh White and Maria Glod, "Muhammad Is Executed for Sniper Killing," *Washington Post,* November 11, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/11/10/AR2009111001396.html.
21. "Jury Convicts Malvo of Sniper Murder," CNN.
22. Stephen Manning, "Malvo Gets Life in 6 Md. Sniper Killings," Associated Press, *Washington Post,* November 8, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/11/08/AR2006110801764.html.

Table 12.2 ▶ Case Snapshot: Colombia's FARC Attacks the US Homeland

Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Red Hat Analysis and Structured Brainstorming	pp. 223, 102	Assessment of Cause and Effect, Idea Generation
Multiple Scenarios Generation	p. 144	Scenarios and Indicators
Indicators	p. 149	Scenarios and Indicators
Indicators Validator™	p. 157	Scenarios and Indicators

12 Colombia's FARC Attacks the US Homeland
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

The challenge for analysts in this case is to convert a very generalized threat warning ("The FARC intends to launch an attack on the US homeland") into an analytic framework that field operators and policy makers can use to protect the nation from a possible terrorist attack. The following exercises walk students through an analytic process that uses Red Hat Analysis, Structured Brainstorming, Multiple Scenarios Generation, Indicators, and the Indicators Validator™ to anticipate how the adversaries are most likely to behave, outline a set of the most likely terrorist courses of action, recognize the signs that the enemy is beginning to implement a particular course of action, and tailor a set of collection requirements for specific field elements.

This case puts students in the shoes of FBI, law enforcement, or Homeland Security analysts who would work this type of case. Students should be advised that the case itself is rooted in fact—the history and tactics described in the text are true. Also, while the threat posited in the case is fictitious, it mimics reality in which specific warning notices are rare and analysts under tight time constraints must work rapidly to direct collection assets and provide decision makers with timely, actionable analysis that can mean the difference between averting disaster or not.

TECHNIQUE 1: RED HAT ANALYSIS AND STRUCTURED BRAINSTORMING

The major victory of the Colombian army and its US military supporters in Colombia against the FARC has created a new situation wherein the FARC sees itself substantially weakened, increasingly desperate, and determined to demonstrate that it is not a spent force. The FARC had threatened to retaliate against the United States in the past for interfering in the internal affairs of Colombia, and its leaders have concluded that the time has come. In this fictitious scenario, members of the Secretariat and top military commanders gather in the Amazon jungle to formulate a strategy for a retaliatory strike in the United States.

The challenge for US analysts is to forecast how an attack is most likely to be launched and, in so doing, help federal, state, local, and tribal officials prevent or mitigate the damage of such an attack. When confronted with this challenge, the first reaction of many students is to propose that the US government issue a general alert to all state, local, and tribal officials that a FARC attack on the homeland may be imminent, and ask them to look out for any suspicious activity that would indicate a FARC attack is being planned or implemented. Unfortunately, such guidance is so unspecific as to lack value for law enforcement officials. The purpose of this exercise is to show that with the use of structured analytic techniques, analysts can generate a plausible set of attention-deserving scenarios and create tailored lists of collection requirements that provide operational value to headquarters, FBI field offices, and fusion centers.

Task 1.

Conduct a Red Hat/Structured Brainstorming exercise to identify the forces and factors that would most influence a FARC decision to attack the US homeland.[1]

Step 1: Gather a group of analysts with knowledge of the FARC Secretariat; operating environment; and senior decision makers' personality, motives, and style of thinking.

It is helpful to include in the brainstorming group both experts on the topic and generalists who can provide more diverse perspectives. When only those working the issue are

included, often the group's perspective is limited to the stream of reporting it reads every day; as a result, key assumptions may remain unchallenged, and historical analogies may be ignored.

Step 2: Pass out sticky notes and marker-type pens to all participants. Inform the team that there is no talking during the sticky-notes portion of the brainstorming exercise.

Use different color sticky notes and encourage the participants to write down short phrases consisting of three to five words, not long sentences.

Step 3: Present the team with the following question: If you were in the FARC Secretariat, what are all the things you personally would think about when planning an attack on the US homeland? The reason for first asking group members how they would react is to establish a baseline for assessing whether the adversary is likely to react differently.

Keep the question as general as possible so as not to inadvertently restrict the creative brainstorming process. It also helps to ask the group if they understand the question and whether they believe it should be worded differently. Spending a few minutes to ensure that everyone understands what the question means is always a good investment.

Ask them to put themselves in the FARC's shoes and simulate how its leaders would respond. Emphasize the need to avoid mirror imaging. The question is not "What would you do if you were in their shoes?" but "How would the FARC leadership approach this problem, given their background, past experience, and the current situation?" It is important to emphasize the importance of avoiding mirror imaging. In a classroom situation, many students may not know much about the FARC; this is why it is important to ensure that all participants read the case study with the relevant background material carefully. They should also have the case study at hand for quick reference.

Step 4: Ask the group to write down responses to the question using a few key words that will fit on a sticky note. After a response is written down, the participant gives it to the facilitator, who then reads it out loud. Marker-type pens are used so that people can easily see what is written on the sticky notes when they are posted on a wall or whiteboard.

Give the students a few minutes to think about the issue and jot down a few ideas. Then go around the room and collect the sticky notes. Read the responses slowly and stick them on the wall or the whiteboard as you read them. Some sample sticky notes might address topics such as financing, type of weapon, target, deniability, need for contacts in the United States, escape plan, motive, logistic support, infiltration, partners, and access to technology.

Step 5: Post all the sticky notes on a wall in the order in which they are called out. Treat all ideas the same. Encourage participants to build on one another's ideas. Usually there is an initial spurt of ideas followed by pauses as participants contemplate the question. After five or ten minutes there is often a long pause of a minute or so. This slowing down suggests that the group has "emptied the barrel of the obvious" and is now on the verge of coming up with some fresh insights and ideas. Do not talk during this pause, even if the silence is uncomfortable.

Remind the group not to talk during this part of the exercise. It is important for them to hear what others are suggesting, as this might stimulate new ideas for them to jot down. Also take care not to spend too much time talking yourself. The participants need quiet time to think, and it is very important for the instructor not to interrupt their thought processes. Often when it is the quietest, the best thinking is taking place.

Step 6: After two or three long pauses, conclude this divergent thinking phase of the brainstorming session.

Step 7: Ask all participants (or a small group) to go up to the wall and rearrange the sticky notes by affinity groups (groups that have some common characteristics). Some sticky notes may be moved several times; some may also be copied if the idea applies to more than one affinity group.

If only a subset of the group goes to the wall to rearrange the sticky notes, then ask those who are remaining in their seats to form into small groups and come up with a list of key drivers or dimensions of the problem based on the themes they heard emerge when the instructor was reading out the sticky notes. This keeps everyone busy and provides a useful check on what is generated by those working at the wall.

Step 8: When all sticky notes have been arranged, ask the group to select a word or phrase that best describes each grouping.

Four or five themes usually emerge from this part of the exercise.

- A variety of potential targets, including US military installations and particularly USSOUTHCOM in Miami; FBI and DEA facilities, mostly in Washington, D.C., and along the US southern border; and senior US officials, who could be targets of assassinations or kidnappings.

- The type of weapons that might be employed, including the *rompas* that the FARC uses in Colombia, rifles or other small arms, far more sophisticated weapons of mass destruction, and even impure drugs such as cocaine adulterated with poison or some other toxic substance.
- Motives for the attack and the intended consequences, including direct military retaliation; a desire to terrorize the broader US population; a hope that creating major economic damage could divert US attention from Colombia; or pure revenge, which could be satisfied by assassinating a senior official.
- Logistic considerations, including how to fund an operation, infiltrate operatives into the United States, identify support networks within the United States, create appropriate documents, and devise effective escape plans once an operation has been completed.
- Whether FARC will seek the assistance of others in designing and implementing the attack. If a sophisticated attack is under consideration, then FARC might require experts in chemical, biological, radiological, or nuclear warfare (CBRN). It might also look to known past partners such as the IRA or Spain's ETA for expertise in planning a terrorist attack against a sophisticated Western nation. Lastly, FARC could reach out to established drug distribution networks already operating within the United States.

Step 9: Ask the group to articulate how, taking all these factors into consideration, they would have orchestrated an attack and to explain why they think they would behave that way. Ask them to list what core values or core assumptions were motivating their behavior or actions. Again, this step establishes a baseline for assessing why the FARC Secretariat is likely to react differently from you and the other members of your group.

Step 10: Once the group can explain in a convincing way why it chose to act the way it did, ask the group members to put themselves in the shoes of the FARC Secretariat and simulate how it would respond, repeating Steps 4 to 8. Emphasize the need to avoid mirror imaging. The question is not "What would you do if you were in their shoes?" but "How would the FARC leadership approach this problem, given their background, past experience, and the current situation?"

Step 11: Once all the sticky notes have been arranged on the board, look for sticky notes that do not fit neatly into any of the groups. Consider whether such an outlier is useless noise or the germ of an idea that deserves further attention.

Often one or two "outlier" sticky notes are worth pointing out to the class because they provide a fresh perspective or suggest a potentially valuable new line of inquiry. Here are some examples:

- A note that says "heroin" could open the door to a discussion of whether the FARC would consider operations to corrupt heroin currently being supplied in the United States to force drug addicts to switch to cocaine as a safer drug of choice.
- A note that says "attack the US embassy in Bogotá" might be initially rejected as outside the scope of the original question, but the instructor should note that by raising the question of an attack on the US embassy, the participant has, in effect, challenged a key assumption of the exercise (that the attack would take place on US soil), and perhaps in the real world this might prompt the group to conduct a key assumptions check and subject this particular assumption to more careful scrutiny.

Step 12: Assess what the group has accomplished. Can you identify four or five key factors, forces, themes, or dimensions that are most likely to influence how the FARC leadership would mount an attack?

Work with the group to develop a consensus on four themes that emerge as the most important drivers for this topic. Write the candidate drivers on the board and draw a line under each driver. The line represents the spectrum for that driver. Label the end points of the spectrum for each dimension or driver being considered. For example, if one driver is "sophistication of the weapon," then at the right end of the line you would write "CBRN" or "WMD" and at the left end of the line you would write "small arms" or "simple weapons" or "rifle."

The themes that most often are generated by this stage of the exercise are as follows:

- Sophistication of weapons (simple such as a rifle or an assassination to highly sophisticated such as a CBRN-type attack).
- Motive (straightforward revenge to terrorizing US population).
- Target (tactical such as a US military base to strategic such as the Pentagon or senior Washington officials).

- Partners (a "do it alone" operation to partnering with other terrorist groups such as the IRA or ETA or obtaining the support of drug distribution networks in the United States).

Other themes that might emerge but usually do not work as well when conducting a Multiple Scenarios Generation exercise include these:

- Cost/benefit (minimal or major commitment of resources and personnel).
- Infiltration/exfiltration (whether to infiltrate FARC operatives or "contract out" to drug networks or radical extremists already operating in the United States).
- Willingness to accept risk (Are FARC leaders willing to consider a spectacular operation that could spur the United States to launch a major retaliatory strike in Colombia, or would they opt for a more modest attack that sends a message but reduces the prospects of a retaliatory strike against their forces?).
- Timing (Will the attack be a quick response easily tied to recent events in Colombia or a much better planned and more sophisticated attack that could take months or even years to pull off?).
- Target security (Will the FARC go after hard or soft targets?).

Step 13: At this point, the group should ask, "Does the FARC Secretariat share our values or motives or methods of operation?" If not, then how do those differences lead them to act in ways we might not have anticipated before engaging in this exercise?

Step 14: Present the results, describing the alternatives that were considered and the rationale for selecting the path the group believes the FARC Secretariat is most likely to take. Consider less conventional means of presenting the results of the analysis, such as the following:

- Describing a hypothetical conversation in which the Secretariat leaders would discuss the issue in the first person.
- Drafting a document (set of instructions, military orders, or directives) that the FARC Secretariat would likely generate.

In most cases, the group should end up with a presentation that defines some version of the following four key drivers and associated spectrums: type of weapon, motive for the attack, target of the attack, and whether any outside assistance is sought.

Students should be encouraged to present their key findings by speaking in the first person, as if they were actual FARC members planning the attack.

Analytic Value Added: The silent structured brainstorming approach is a powerful technique to pull out new and often never previously considered ideas and concepts. It avoids the trap of deferring to the most knowledgeable person in the room by giving everyone an equal, but silent, opportunity to surface ideas. While conducting the structured brainstorming exercise, it is useful to note whether particularly useful and creative ideas are generated after long pauses when everyone is thinking; if this does occur, it is important to alert the entire group to the phenomenon.

Were we careful to avoid mirror imaging when we put ourselves "in the shoes" of the FARC Secretariat? By putting themselves in the "shoes" of the FARC, analysts are more likely to focus on attack scenarios the FARC would be best positioned to implement successfully and thus be the most likely. By conducting a Red Hat Analysis, they usually focus not only on how to launch an attack but the extent to which the plan they choose could make them vulnerable to retaliation. Often exfiltrating forces is as important as infiltrating them into the United States.

Did we explore all the possible forces and factors that could influence how the FARC might launch an attack on the US homeland? The sticky notes should capture a broad spectrum of forces and factors, including logistical preparations, financing, preferred target, type of weapon to employ, ability to maintain operational security, mechanisms for infiltrating and exfiltrating forces, and whether to seek the assistance of or partner with other groups.

Did our ideas group themselves into coherent affinity groups? How did we treat outliers or sticky notes that seemed to belong in a group all by themselves? Did the outliers spark new lines of inquiry? Placing like ideas into affinity groups can be a challenging task; asking those not at the wall to come up with their own categories often provides a useful sanity check. Always take time to give outlier ideas their due attention. Invariably a structured

brainstorming exercise will stimulate ideas that at first appear to be off-the-wall or not directly related to the task. It is useful in the group discussion to ask what prompted the person to prepare that note. Sometimes the explanation will surface an idea or a concept that no one else in the group would have considered. For example, a note that said "submarines" might at first appear odd, but submarines or submersibles are used increasingly to move drugs from Colombia to the United States and it is possible they could be adapted to infiltrate a FARC assassination team.

Did the labels we generated for each group accurately capture the essence of that set of sticky notes? Groups often have difficulty avoiding the trap of assigning obvious labels such as "political, economic, social" or "foreign, domestic." Encourage the students to think beyond these obvious categories by asking a series of Why? or Because? questions.

TECHNIQUE 2: MULTIPLE SCENARIOS GENERATION

In the complex, evolving, uncertain situations that intelligence analysts and decision makers must deal with, the future is not easily predicable. The best an analyst can do is to identify the driving forces that may determine future outcomes and monitor those forces as they interact to become the future. Scenarios are a principal vehicle for doing this. Scenarios are plausible and sometimes provocative stories about how the future might unfold. When alternative futures have been clearly outlined, decision makers can mentally rehearse these futures and ask themselves, "What should I be doing now to prepare for these futures?"

Scenarios Analysis provides a framework for considering various plausible futures. Trying to divine or predict a single outcome typically is a disservice to senior officials and decision makers. Generating several scenarios helps focus attention on the key underlying forces and factors most likely to influence how a situation develops. Multiple Scenarios Generation creates a large number of possible scenarios. This is desirable to make sure nothing has been overlooked. Once generated, the scenarios can be screened quickly, without detailed analysis of each one. Once sensitized to these different scenarios, analysts are more likely to pay attention to outlying data that would suggest that events are playing out in a way not previously imagined.

Task 2.

Use Multiple Scenarios Generation to identify the most plausible attack scenarios the FARC would consider in launching a retaliatory attack on the US homeland.

Step 1: Clearly define the focal issue and the specific goals of the futures exercise.

When you have little intelligence on a specific threat but substantial information on the potential perpetrator, Multiple Scenarios Generation is a useful tool to scope the problem, think creatively about potential attack scenarios, and generate actionable intelligence. In this case, the focal question is "What are the most plausible ways the FARC would mount an attack on the US homeland?" The goal of the exercise is to use the four key drivers selected in the Red Hat/Structured Brainstorming Exercise first to generate a multitude of possible attack scenarios and then to select the scenarios that seem the most plausible, thus deserving the attention of those responsible for thwarting or mitigating the consequences of such an attack.

Step 2: Brainstorm to identify the key forces, factors, or events that are most likely to influence how the issue will develop over a specified time period. In this case, use the four or five key drivers, themes, or dimensions that emerged from Task 1, the Red Hat/Structured Brainstorming exercise.

In Task 1, four key drivers emerged: the type of weapon, the motive for the attack, the most likely target of an attack, and whether outside assistance will be sought.

Step 3: For each of these key drivers, define the two ends of the spectrum.

For the purposes of illustration, the spectrums can be defined as follows:

A. Weapon (simple weapon such as a rifle to a highly sophisticated CBRN attack).

B. Motive (retaliation for recent military operation in Colombia to much broader aim to terrorize the US population).

C. Target (tactical attack on a US military base to the strategic targeting of a senior Washington official).

D. Partners (a "do it alone" operation or partnering with the IRA).

Step 4: Pair the drivers in a series of 2 × 2 matrices. If you have four drivers, they can be combined into six pairs,

generating six different matrices. Five drivers would generate ten different matrices.

In this case study, the pairs used to form the six matrices would be: AB (weapon/motive), AC (weapon/target), AD (weapon/partner), BC (motive/target), BD (motive/partner), and CD (target/partner). The class usually is broken into smaller groups to work each 2 × 2 matrix. With six matrices, it usually works best to assign two matrices to each of three groups. Be careful in assigning the matrices to give each group the opportunity to think about all of the drivers. This can be accomplished by assigning the matrices as follows: Group 1 (AB and CD), Group 2 (AC and BD), and Group 3 (AD and BC).

Step 5: Develop a story or two for each quadrant of each 2 × 2 matrix.

For example, Group 2 was asked to come up with four stories (one story for each quadrant of the matrix) for AC (weapon/target). Their work might look like Figure 9.2, in which the *x*-axis represents a tactical versus a strategic target and the *y*-axis represents the spectrum of simple to sophisticated weapons. In each matrix, the students have brainstormed a potential attack scenario. For example, a tactical attack using weapons of mass destruction could involve a biological attack on the water supply of a military base that was supporting US military operations in Colombia. In another quadrant, a simple attack designed to terrorize the US population could be the kidnapping of the son or daughter of a chief of police of a major metropolitan area such as Miami. The students opted to propose the kidnapping of a child because it was assumed a child would be a soft target unlikely to have security protection.

If one group works more quickly than the others, the instructor can ask the group to start putting together lists of indicators for their favorite scenarios.

Students should present similar matrices for all six combinations of drivers. Once all the matrices have been presented and discussed, the class should look for themes that emerge or seem to repeat in several of the matrices. These may be more deserving of attention if similar ideas were generated by different groups independently. Students should also discuss which of the scenarios are most deserving of the attention of US policy makers and law enforcement officials and provide reasons to support their choices.

Step 6: From all the scenarios generated, select three or four that are the most deserving of attention because they best illustrate the range of attacks the FARC is most likely to contemplate.

After some discussion, the class can either reach consensus on the top four scenarios to consider, or it can vote to identify the most attention-deserving scenarios. The group should endeavor to select a set of scenarios that best defines the most likely attack space. When two scenarios appear to be very similar, then they should be combined.

The standard rule is to give participants one vote for every three things being considered. In this instance, if twenty-four different scenarios were generated, each participant would be allowed to vote for the eight scenarios he or she deemed most deserving of attention. The scenarios with the most votes would be the lead candidates to present to the customer.

Some sample scenarios that might be generated include these:

- Use *rompas* to attack USSOUTHCOM's headquarters in Miami.
- Conduct a sniper attack on US counterdrug officials or military officers associated with operations in Colombia.
- Contaminate the food supply or water supply of a US military base supporting anti-FARC operations in Colombia.
- Enlist the support of the IRA to conduct a targeted bombing aimed at the Colombian ambassador to the United Nations or the Colombian ambassador in Washington, D.C. The FARC assassins could be dressed as Colombian military officers with IRA operatives providing logistic support.
- Kill as many American drug users as possible to terrorize the US population and send a clear message not to fool with the FARC and Colombia.

Step 7: Consider whether one of the final scenarios you select might be described as a "wild card" (low-probability/high-impact) or "nightmare" scenario.

Although plausibility is a major criterion for selecting the most attention-deserving scenarios, there are times when a highly unlikely scenario still should be included in the final set of four because albeit unlikely, the consequences for the United States would be severe and senior policy makers should be alerted to the possibility, however remote. An illustration of how four scenarios might be selected is provided in Figure 12.4.

Figure 12.3 ▶ Multiple Scenarios Generation: Sample Matrix of FARC Attack on the US Homeland

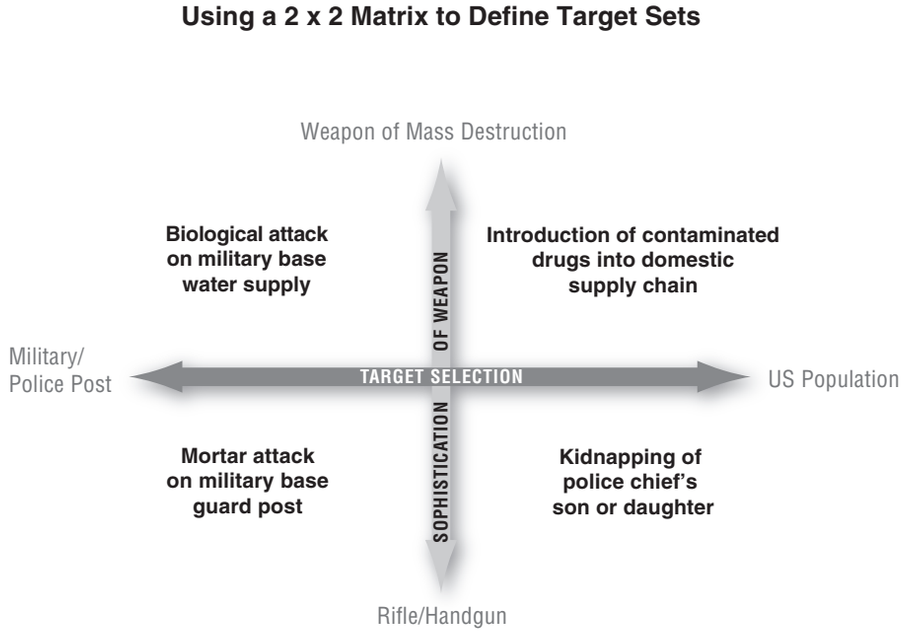
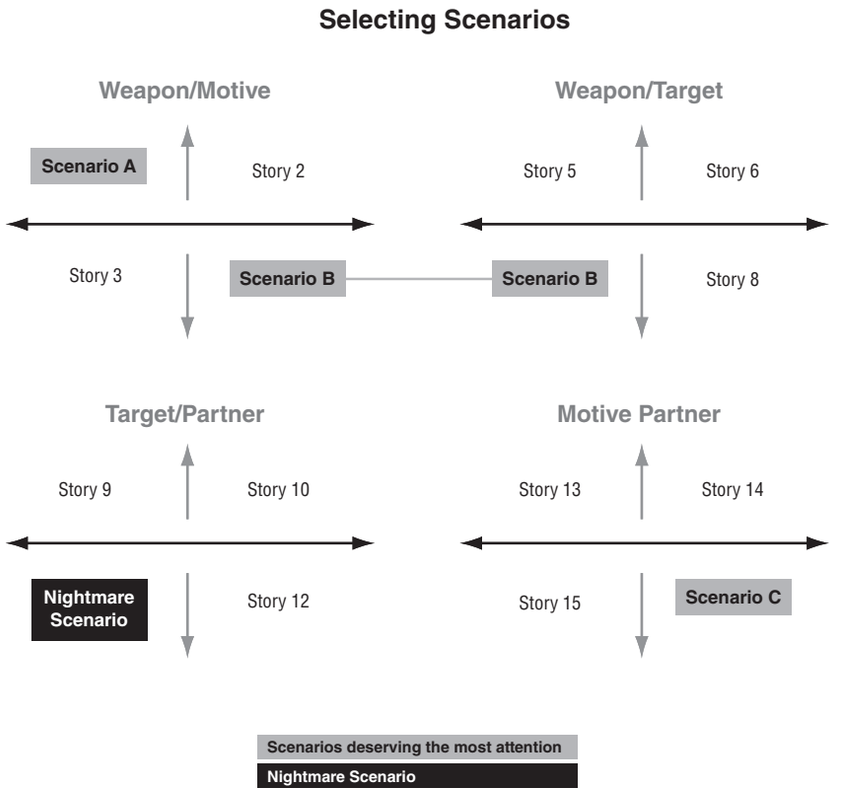


Figure 12.4 ▶ Multiple Scenarios Generation: Selecting the Most Attention-Deserving Scenarios of a FARC Attack on the US Homeland



Some possible wildcard or nightmare scenarios that might be generated from this exercise would be these:

- A decision by the FARC leadership to pay drug distributors within the United States to spike illegal drugs with a highly toxic substance and distribute them in communities that surround US military bases that have deployed troops to Colombia.
- An attempt by FARC members to assassinate the administrator or assistant administrator of the Drug Enforcement Administration.

Analytic Value Added: **Did the technique help us generate a robust set of potential scenarios to consider?** The Multiple Scenarios Generation technique can be a powerful tool to generate new ideas and attack scenarios that might never have been considered as part of a traditional analysis.

Did we discover new scenarios that we probably would not have imagined if we had not used this particular technique? The technique forces analysts to reframe the question in many different ways; often the combinations prompt totally new ways of defining the threat environment. The approach should give analysts more confidence that they have captured the entire threat space and some assurance that they are less likely to be surprised by how events actually play out.

Did similar themes emerge from different matrices even though different pairs of drivers were being considered? When similar themes emerge from more than one matrix, analysts can be more confident that a key dimension has been captured that may require the attention of the decision makers.

Were the final scenarios selected both plausible and the most deserving of attention? The exercise helps analysts avoid the frequent trap of coming to premature closure and focusing on the one or two plausible scenarios that first come to mind. In selecting the most attention-deserving scenarios, it is always helpful to work from a previously agreed upon set of key criteria.

TECHNIQUE 3: INDICATORS

Indicators are observable or deduced phenomena that can be periodically reviewed to help track events, distinguish between competing hypotheses, spot emerging trends, and warn of unanticipated change. An indicators list is a preestablished set of actions, conditions, facts, or events whose simultaneous occurrence would argue strongly that a phenomenon is present or a hypothesis is correct. The identification and monitoring of indicators are fundamental tasks of intelligence analysis because they are the principal means of avoiding surprise. In intelligence analysis, indicators are often described as predictive indicators that look forward. In the law enforcement community, indicators are used to assess whether a target's activities or behavior are consistent with an established pattern or lead hypothesis. These are often described as descriptive indicators that look backward.

Preparation of a detailed indicator list by a group of knowledgeable analysts is usually a good learning experience for all participants. It can be a useful medium for an exchange of knowledge between analysts from different organizations or those with different types of expertise—for example, counterterrorism or counterdrug analysis, infrastructure protection, and country expertise. The indicator list can become the basis for conducting an investigation or directing collection efforts and routing relevant information to all interested parties. Identification and monitoring of indicators or signposts that a scenario is emerging can provide early warning of the direction in which the future is heading, but these early signs are not obvious. The human mind tends to see what it expects to see and to overlook the unexpected. Indicators take on meaning only in the context of a specific scenario with which they have been identified. The prior identification of a scenario and associated indicators can create an awareness that prepares the mind to recognize and prevent a bad scenario from unfolding or help a good scenario to come about.

Task 3.

Create separate sets of indicators for each alternative scenario that was generated in Task 2.

Step 1: Work alone, or preferably with a small group, to brainstorm a list of indicators for each scenario.

For the purposes of illustrating this case study, we have generated indicators for the following four scenarios:

A. Kill as many American drug users as possible to terrorize the US population and send a clear message not to fool with the FARC and Colombia.

B. Use *rompas* to attack USSOUTHCOM's headquarters in Miami.

C. Enlist the support of the IRA to conduct a targeted bombing aimed at the Colombian ambassador to the UN or the Colombian ambassador in Washington, D.C. The FARC assassins could be dressed as Colombian military officers with IRA operatives providing logistic support.

Table 12.5 ▶ FARC Attack on the US Homeland: Indicators List

Number	Indicator
	Scenario A: FARC poisons cocaine to terrorize US population.
A-1	DEA chemists see increase in reports of cocaine laced with toxic substance in several major cities.
A-2	Border police report fewer seizures of bulk cash heading south.
A-3	Informants report a "buzz" on the street to avoid purchases of cocaine.
A-4	There is an unusual spike in reported drug overdoses in several cities.
A-5	Drug informants talk of "special payoffs" to local drug distributors.
A-6	The FARC posts statements on the Internet saying it will retaliate against the United States for supporting Colombian military strikes against FARC guerrillas.
A-7	Urban drug treatment centers receive queries about what substances are most often mixed with cocaine to increase volume and profits.
A-8	Drug mules are carrying smaller amounts of cash back to Colombia.
A-9	Communications increase between US drug distributors and Latin America.
A-10	Local US law enforcement reports increased bulk purchases of poisonous substances such as arsenic.
	Scenario B: FARC uses *rompas* to launch mortar attack on USSOUTHCOM headquarters in Miami.
B-1	USSOUTHCOM security reports suspicious cars seen loitering on streets in vicinity of headquarters.
B-2	Analysts looking at FARC Internet site report claims that FARC will make the US military pay for its misdeeds.
B-3	Hispanic males are observed taking photos of USSOUTHCOM headquarters from a distance.
B-4	Suspicious purchases of liquid petroleum gas containers are noted in Miami hardware stores.
B-5	US government sources report that Venezuela has provided documents and passports to FARC operatives to facilitate their international travel.
B-6	Recent FARC guerrilla defectors mention a mock-up building in the Amazon is being used for target practice with *rompas*.
B-7	USSOUTHCOM employees tell their supervisors that they are being approached by strangers and asked who works where in the complex.
B-8	An increased number of mortar attacks using *rompas* is reported in Colombia.
	Scenario C: FARC assassinates Colombian ambassadors with IRA support.
C-1	There are reports of FARC meetings and communications with the IRA.
C-2	FARC publishes open letter to the US president stating that FARC will not be intimidated by actions of the US military.
C-3	Kidnappings of field-grade Colombian military officers in Colombia surge.
C-4	There are intelligence reports of IRA hit squads being dispatched to North America.
C-5	Defecting FARC guerrillas report talk of a big operation "up north."
C-6	Colombians in New York report suspicious persons loitering outside the mission offices.
C-7	FARC Internet site claims that FARC will make the US military pay for its misdeeds.
C-8	Suspected FARC members entering the United States are found in possession of Colombian military uniforms.
C-9	A FARC informant reports that a special squad is being formed for a major operation.
	Scenario D: Marijuana laced with poison kills many in the vicinity of US military bases.
D-1	Street informants report a "buzz" in the Hispanic community that the FARC is planning a special operation in the United States.
D-2	Local drug dealers say they are being surveyed by people up their distribution chain asking for details on their user populations.
D-3	Local health officials report an increase in drug-related deaths among teenagers.
D-4	DEA chemists report an increase in marijuana laced with arsenic and other toxic substances.
D-5	Street informants report that their suppliers are talking about making easy money.
D-6	A new theme emerges on Facebook that marijuana consumption may be more dangerous than most suspect.
D-7	Analysts note postings by FARC on its Internet site stating that the United States will pay dearly for violating Colombian sovereignty.
D-8	Drug users become increasingly anxious that the drugs they might purchase could be contaminated.

D. Pay drug distributors within the United States to lace marijuana sold mostly to teenagers with a highly toxic, lethal substance and distribute it to communities that surround US military bases that have deployed troops to Colombia.

A brainstorming session generated the indicators shown in Table 12.5 for each scenario.

Step 2: Review and refine each set of indicators, discarding any that are duplicative within any given scenario and combining those that are similar.

In this example, C-5 and C-9 are similar and merit combination into a new indicator: "FARC informants or defectors report that a special squad is being formed for a major operation up north." Similarly, C-2 and C-7 should be combined to state: "FARC warns the United States publicly that it will no longer tolerate American interference in Colombia's internal affairs, particularly with its military forces."

Step 3: Examine each indicator to determine whether it meets the following five criteria. Discard those that are found wanting.

1. **Observable and collectible**. There must be some reasonable expectation that, if present, the indicator will be observed and reported by a reliable source. If an indicator will be used to monitor change over time, it must be collectible over time.
2. **Valid**. An indicator must be clearly relevant to the endstate the analyst is trying to predict or assess, and it must be inconsistent with all or at least some of the alternative explanations or outcomes. It must accurately measure the concept or phenomenon at issue.
3. **Reliable**. Data collection must be consistent when comparable methods are used. Those observing and collecting data must observe the same things. Reliability requires precise definition of the indicators.
4. **Stable**. An indicator must be useful over time to allow comparisons and to track events. Ideally, the indicator should be observable early in the evolution of a development so that analysts and decision makers have time to react accordingly.
5. **Unique**. An indicator should measure only one thing and, in combination with other indicators, should point only to the phenomenon being studied. Valuable indicators are those that are not only consistent with a specified scenario or hypothesis but are also inconsistent with all other alternative scenarios.

In this case study:

- A-8 should be dropped from the list because it fails the test as an observable and collectible indicator. Few mules are intercepted taking money back to Colombia, and it would be very difficult to know if the total volume of cash moving from the United States to the drug lords in Colombia was diminishing.
- A-9 fails two tests: it is neither unique nor valid. It needs to be rewritten as follows: "New communications are identified between FARC leaders and drug distributors in the United States."
- B-4 is not valid because it lacks specificity. It should be rewritten to state: "Known FARC sympathizers are reported purchasing suspicious quantities of liquid petroleum gas canisters."
- D-8 fails the test of an observable and collectible indicator. It should be rewritten to state: "Informants report that drug users are complaining that the drugs they are purchasing may be contaminated."

A revised list of indicators is presented in Table 12.6.

Analytic Value Added: **What new or otherwise implicit criteria did the indicators process expose?** Students' answers will vary according to the specifics of their indicator sets. However, a good indicator set should help the analyst identify explicit criteria for tracking and judging the course of events. Often it is useful to note that it is easy to generate indicators for some scenarios, such as a mortar attack on USSOUTHCOM headquarters that involves surveillance activity and the acquisition or importation of weaponry, and difficult for others, such as an assassination plot.

Do the indicators prompt additional areas for collection? This will vary according to the students' indicator sets. However, a well-conceived set of indicators should become the basis for directing collection efforts and for routing relevant information to all interested parties in several US government agencies.

TECHNIQUE 4: INDICATORS VALIDATOR™

The Indicators Validator™ is a simple tool for assessing the diagnostic power of indicators. Once an analyst has developed a set of attention-deserving alternative scenarios or competing hypotheses, the next step is to generate indicators for each scenario or hypothesis that would appear if that particular

Table 12.6 ▶ FARC Attack on the US Homeland: Revised Indicators

Number	Indicator
	Scenario A: FARC poisons cocaine to terrorize US population.
A-1	DEA chemists see increase in reports of cocaine laced with toxic substance in several major cities.
A-2	Border police report fewer seizures of bulk cash heading south.
A-3	Informants report a "buzz" on the street to avoid purchases of cocaine.
A-4	There is an unusual spike in reported drug overdoses in several cities.
A-5	Drug informants talk of "special payoffs" to local drug distributors.
A-6	The FARC posts statements on the Internet saying it will retaliate against the United States for supporting Colombian military strikes against FARC guerrillas.
A-7	Urban drug treatment centers receive queries about what substances are most often mixed with cocaine to increase volume and profits.
A-8	New communications are identified between FARC leaders and drug distributors in the United States.
A-9	Local US law enforcement reports increased bulk purchases of poisonous substances such as arsenic.
	Scenario B: FARC uses *rompas* to launch mortar attack on USSOUTHCOM headquarters in Miami.
B-1	USSOUTHCOM security reports suspicious cars seen loitering on streets in vicinity of headquarters.
B-2	Analysts looking at FARC Internet site report claims that FARC will make the US military pay for its misdeeds.
B-3	Hispanic males are observed taking photos of USSOUTHCOM headquarters from a distance.
B-4	Known FARC sympathizers are reported purchasing suspicious quantities of liquid petroleum gas canisters.
B-5	US government sources report that Venezuela has provided documents and passports to FARC operatives to facilitate their international travel.
B-6	Recent FARC guerrilla defectors mention a mock-up building in the Amazon is being used for target practice with *rompas*.
B-7	USSOUTHCOM employees tell their supervisors that they are being approached by strangers and asked who works where in the complex.
B-8	An increased number of mortar attacks using *rompas* is reported in Colombia.
	Scenario C: FARC assassinates Colombian ambassadors with IRA support.
C-1	There are reports of FARC meetings and communications with the IRA.
C-2	FARC warns the United States publicly that it will no longer tolerate American interference in Colombia's internal affairs, particularly with its military forces.
C-3	Kidnappings of field-grade Colombian military officers surge.
C-4	There are intelligence reports of IRA hit squads being dispatched to North America.
C-5	FARC informants or defectors report that a special squad is being formed for a major operation "up north."
C-6	Colombians in New York report suspicious persons loitering outside the mission offices.
C-7	Suspected FARC members entering the United States are found in possession of Colombian military uniforms.
	Scenario D: Marijuana laced with poison kills many in the vicinity of US military bases.
D-1	Street informants report a "buzz" in the Hispanic community that the FARC is planning a special operation in the United States.
D-2	Local drug dealers say they are being surveyed by people up their distribution chain asking for details on their user populations.
D-3	Local health officials report an increase in drug-related deaths among teenagers.
D-4	DEA chemists report an increase in marijuana laced with arsenic and other toxic substances.
D-5	Street informants report that their suppliers are talking about making easy money.
D-6	A new theme emerges on Facebook that marijuana consumption may be more dangerous than most suspect.
D-7	Analysts note postings by FARC on its Internet site stating that the United States will pay dearly for violating Colombian sovereignty.
D-8	Informants report that drug users are complaining that the drugs they are purchasing are contaminated.

scenario were beginning to emerge or that particular hypothesis were true. A critical question that is not often asked is whether a given indicator would appear only for the scenario or hypothesis to which it is assigned or also in one or more alternative scenarios or hypotheses. Indicators that could appear under several are not considered diagnostic, suggesting that they are not particularly useful in determining whether a specific scenario is beginning to emerge or a particular hypothesis is true. The ideal indicator is highly likely for the scenario to which it is assigned and highly unlikely for all others.

Task 4.

Use the Indicators Validator™ to assess the diagnosticity of your indicators.

Step 1: Create a matrix similar to that used for Analysis of Competing Hypotheses. This can be done manually or by using the Indicators Validator™ software. Contact Globalytica, LLC at THINKSuite@globalytica.com or go to http://www.globalytica.com to obtain access to the Indicators Validator™ software if it is not available on your system. List the alternative scenarios along the top of the matrix and the indicators that have been generated for each of the scenarios down the left side of the matrix.

Step 2: Moving across the indicator rows, assess whether the indicator for each scenario

- Is highly likely to appear
- Is likely to appear
- Could appear
- Is unlikely to appear
- Is highly unlikely to appear

Indicators developed for their particular scenario, the home scenario, should be either highly likely or likely.

If the software is unavailable, you can do your own scoring. If the indicator is highly likely in the home scenario, then in the other scenarios,

- Highly likely is 0 points.
- Likely is 1 point.
- Could appear is 2 points.
- Unlikely is 4 points.
- Highly unlikely is 6 points.

If the indicator is likely in the home scenario, then in the other scenarios,

- Highly likely is 0 points.
- Likely is 0 points.
- Could appear is 1 point.
- Unlikely is 3 points.
- Highly unlikely is 5 points.

Step 3: Tally up the scores across each row, as shown in Table 12.7, and then rank order all the indicators.

Table 12.7 ▶ FARC Attack on the US Homeland: Indicators Validator™ Scoring

Number	Indicator	Scenario A	Scenario B	Scenario C	Scenario D	Score
Scenario A: FARC poisons cocaine to terrorize US population.						
A-1	DEA chemists see increase in reports of cocaine laced with toxic substance in several major cities.	HL	HU (6)	HU (6)	C (2)	14
A-2	Border police report fewer seizures of bulk cash heading south.	L	HU (5)	HU (5)	L (0)	10
A-3	Informants report a "buzz" on the street to avoid purchases of cocaine.	HL	HU (6)	HU (6)	C (2)	14
A-4	There is an unusual spike in reported drug overdoses in several cities.	HL	HU (6)	HU (6)	HL (0)	12
A-5	Drug informants talk of "special payoffs" to local drug distributors.	L	HU (5)	HU (5)	C (1)	11
A-6	The FARC posts statements on the Internet saying it will retaliate against the United States for supporting Colombian military strikes against FARC guerrillas.	HL	HL (0)	HL (0)	HL (0)	0

Table 12.7 ▶ *(Continued)*

Number	Indicator	Scenario A	Scenario B	Scenario C	Scenario D	Score
A-7	Urban drug treatment centers receive queries about what substances are most often mixed with cocaine to increase volume and profits.	L	HU (5)	HU (5)	C (1)	11
A-8	New communications are identified between FARC leaders and drug distributors in the United States.	L	U (3)	U (3)	L (0)	6
A-9	Local US law enforcement reports increased bulk purchases of poisonous substances such as arsenic.	L	HU (5)	HU (5)	L (0)	10
	Scenario B: FARC uses *rompas* to launch mortar attack on USSOUTHCOM headquarters in Miami.					
B-1	USSOUTHCOM security reports suspicious cars seen loitering on streets in vicinity of headquarters.	C (1)	L	C (1)	L (0)	2
B-2	Analysts looking at FARC Internet site report claims that FARC will make the US military pay for its misdeeds.	HL (0)	HL	HL (0)	L (1)	1
B-3	Hispanic males are observed taking photos of USSOUTHCOM headquarters from a distance.	U (4)	HL	C (2)	C (2)	8
B-4	Known FARC sympathizers are reported purchasing suspicious quantities of liquid petroleum gas canisters.	HU (5)	L	U (3)	U (3)	11
B-5	US government sources report that Venezuela has provided documents and passports to FARC operatives to facilitate their international travel.	C (2)	HL	HL (0)	C (2)	4
B-6	Recent FARC guerrilla defectors mention a mock-up building in the Amazon is being used for target practice with *rompas*.	U (3)	L	C (1)	U (3)	7
B-7	USSOUTHCOM employees tell their supervisors that they are being approached by strangers and asked who works where in the complex.	U (4)	HL	L (1)	C (2)	7
B-8	An increased number of mortar attacks using *rompas* is reported in Colombia.	HU (6)	HL	C (2)	HU (6)	14
	Scenario C: FARC assassinates Colombian ambassadors with IRA support.					
C-1	There are reports of FARC meetings and communications with the IRA.	U (4)	C (2)	HL	U (4)	10
C-2	FARC warns the United States publicly that it will no longer tolerate American interference in Colombia's internal affairs, particularly with its military forces.	L (1)	HL (0)	HL	L (1)	2
C-3	Kidnappings of field-grade Colombian military officers surge.	U (4)	C (2)	HL	U (4)	10
C-4	There are intelligence reports of IRA hit squads being dispatched to North America.	U (4)	C (2)	HL	U (4)	10
C-5	FARC informants or defectors report that a special squad is being formed for a major operation "up north."	U (3)	L (0)	L	U (3)	6
C-6	Colombians in New York report suspicious persons loitering outside the mission offices.	U (4)	U (4)	HL	U (4)	12
C-7	Suspected FARC members entering the United States are found in possession of Colombian military uniforms.	U (4)	U (4)	HL	U (4)	12
	Scenario D: Marijuana laced with poison kills many in the vicinity of US military bases.					
D-1	Street informants report a "buzz" in the Hispanic community that the FARC is planning a special operation in the United States.	C (1)	C (1)	U (3)	L	5

(Continued)

Table 12.7 ▶ FARC Attack on the US Homeland: Indicators Validator™ Scoring *(Continued)*

Number	Indicator	Scenario A	Scenario B	Scenario C	Scenario D	Score
D-2	Local drug dealers say they are being surveyed by people up their distribution chain asking for details on their user populations.	C (1)	U (3)	U (3)	L	7
D-3	Local health officials report an increase in drug-related deaths among teenagers.	L (0)	U (3)	U (3)	L	6
D-4	DEA chemists report an increase in marijuana laced with arsenic and other toxic substances.	C (2)	U (4)	U (4)	HL	10
D-5	Street informants report that their suppliers are talking about making easy money.	L (0)	U (3)	U (3)	L	6
D-6	A new theme emerges on Facebook that marijuana consumption may be more dangerous than most suspect.	C (2)	U (4)	U (4)	HL	10
D-7	Analysts note postings by FARC on its Internet site stating that the United States will pay dearly for violating Colombian sovereignty.	HL (0)	HL (0)	HL (0)	HL	0
D-8	Informants report that drug users are complaining that the drugs they are purchasing are contaminated.	HL (0)	U (4)	U (4)	HL	8

Note: HL = highly likely to appear; L = likely to appear; C = could appear; U = unlikely to appear; HU = highly unlikely to appear.

Step 4: Re-sort the indicators, putting those with the highest total scores at the top of the matrix and those with the lowest scores at the bottom (Table 12.8). The most discriminating indicator is highly likely to emerge under the home scenario and highly unlikely to emerge under all other scenarios. The least discriminating indicator is

Table 12.8 ▶ FARC Attack on the US Homeland: Rank Ordering of the Indicators on the Basis of Diagnosticity

Number	Indicator	Scenario A	Scenario B	Scenario C	Scenario D	Score
A-1	DEA chemists see increase in reports of cocaine laced with toxic substance in several major cities.	HL	HU (6)	HU (6)	C (2)	14
A-3	Informants report a "buzz" on the street to avoid purchases of cocaine.	HL	HU (6)	HU (6)	C (2)	14
B-8	An increased number of mortar attacks using *rompas* is reported in Colombia.	HU (6)	HL	C (2)	HU (6)	14
A-4	There is an unusual spike in reported drug overdoses in several cities.	HL	HU (6)	HU (6)	HL (0)	12
C-6	Colombians in New York report suspicious persons loitering outside the mission offices.	U (4)	U (4)	HL	U (4)	12
C-7	Suspected FARC members entering the United States are found in possession of Colombian military uniforms.	U (4)	U (4)	HL	U (4)	12
A-5	Drug informants talk of "special payoffs" to local drug distributors.	L	HU (5)	HU (5)	C (1)	11
A-7	Urban drug treatment centers receive queries about what substances are most often mixed with cocaine to increase volume and profits.	L	HU (5)	HU (5)	C (1)	11
B-4	Known FARC sympathizers are reported purchasing suspicious quantities of liquid petroleum gas canisters.	HU (5)	L	U (3)	U (3)	11
A-2	Border police report fewer seizures of bulk cash heading south.	L	HU (5)	HU (5)	L (0)	10
A-9	Local US law enforcement reports increased bulk purchases of poisonous substances such as arsenic.	L	HU (5)	HU (5)	L (0)	10

Table 12.8 ▶ *(Continued)*

Number	Indicator	Scenario A	Scenario B	Scenario C	Scenario D	Score
C-1	There are reports of FARC meetings and communications with the IRA.	U (4)	C (2)	HL	U (4)	10
C-3	Kidnappings of field-grade Colombian military officers surge.	U (4)	C (2)	HL	U (4)	10
C-4	There are intelligence reports of IRA hit squads being dispatched to North America.	U (4)	C (2)	HL	U (4)	10
D-4	DEA chemists report an increase in marijuana laced with arsenic and other toxic substances.	C (2)	U (4)	U (4)	HL	10
D-6	A new theme emerges on Facebook that marijuana consumption may be more dangerous than most suspect.	C (2)	U (4)	U (4)	HL	10
B-3	Hispanic males are observed taking photos of USSOUTHCOM headquarters from a distance.	U (4)	HL	C (2)	C (2)	8
D-8	Informants report that drug users are complaining that the drugs they are purchasing are contaminated.	HL (0)	U (4)	U (4)	HL	8
B-6	Recent FARC guerrilla defectors mention a mock-up building in the Amazon is being used for target practice with *rompas*.	U (3)	L	C (1)	U (3)	7
B-7	USSOUTHCOM employees tell their supervisors that they are being approached by strangers and asked who works where in the complex.	U (4)	HL	L (1)	C (2)	7
D-2	Local drug dealers say they are being surveyed by people up their distribution chain asking for details on their user populations.	C (1)	U (3)	U (3)	L	7
A-8	New communications are identified between FARC leaders and drug distributors in the United States.	L	U (3)	U (3)	L (0)	6
C-5	FARC informants or defectors report that a special squad is being formed for a major operation "up north."	U (3)	L (0)	L	U (3)	6
D-3	Local health officials report an increase in drug-related deaths among teenagers.	L (0)	U (3)	U (3)	L	6
D-5	Street informants report that their suppliers are talking about making easy money.	L (0)	U (3)	U (3)	L	6
D-1	Street informants report a "buzz" in the Hispanic community that the FARC is planning a special operation in the United States.	C (1)	C (1)	U (3)	L	5
B-5	US government sources report that Venezuela has provided documents and passports to FARC operatives to facilitate their international travel.	C (2)	HL	HL (0)	C (2)	4
B-1	USSOUTHCOM security reports suspicious cars seen loitering on streets in vicinity of headquarters.	C (1)	L	C (1)	L (0)	2
C-2	FARC warns the United States publicly that it will no longer tolerate American interference in Colombia's internal affairs, particularly with its military forces.	L (1)	HL (0)	HL	L (1)	2
B-2	Analysts looking at FARC Internet site report claims that FARC will make the US military pay for its misdeeds.	HL (0)	HL	HL (0)	L (1)	1
A-6	The FARC posts statements on the Internet saying it will retaliate against the United States for supporting Colombian military strikes against FARC guerrillas.	HL	HL (0)	HL (0)	HL (0)	0
D-7	Analysts note postings by FARC on its Internet site stating that the United States will pay dearly for violating Colombian sovereignty.	HL (0)	HL (0)	HL (0)	HL	0

Note: HL = highly likely to appear; L = likely to appear; C = could appear; U = unlikely to appear; HU = highly unlikely to appear.

highly likely to appear in all scenarios. Most indicators will fall somewhere in between.

Step 5: The indicators with the most highly unlikely and unlikely ratings are the most discriminating and should be retained.

Step 6: Indicators with no highly unlikely or unlikely ratings should be discarded.

Step 7: Use your judgment as to whether you should retain or discard indicators that score fewer points. Generally, you should discard all indicators that have highly unlikely or unlikely ratings. In some cases, an indicator may be worth keeping if it is useful when viewed in combination with several other indicators.

In this illustration, the following indicators would be discarded: B-5 (4 points), B-1 (2), C-2 (2), B-2 (1), A-6 (0), and D-7 (0). Although D-1 has a score of only 5 points, it is not discarded because it had an unlikely rating in the row.

Step 8: Once nondiscriminating indicators have been eliminated, regroup the indicators under their home scenario (Table 12.9).

Table 12.9 ▶ FARC Attack on the US Homeland: Rank Ordering of the Indicators on the Basis of Diagnosticity by Scenario

Number	Indicator	Scenario A	Scenario B	Scenario C	Scenario D	Score
Scenario A: FARC poisons cocaine to terrorize US population.						
A-1	DEA chemists see increase in reports of cocaine laced with toxic substance in several major cities.	HL	HU (6)	HU (6)	C (2)	14
A-3	Informants report a "buzz" on the street to avoid purchases of cocaine.	HL	HU (6)	HU (6)	C (2)	14
A-4	There is an unusual spike in reported drug overdoses in several cities.	HL	HU (6)	HU (6)	HL (0)	12
A-5	Drug informants talk of "special payoffs" to local drug distributors.	L	HU (5)	HU (5)	C (1)	11
A-7	Urban drug treatment centers receive queries about what substances are most often mixed with cocaine to increase volume and profits.	L	HU (5)	HU (5)	C (1)	11
A-2	Border police report fewer seizures of bulk cash heading south.	L	HU (5)	HU (5)	L (0)	10
A-9	Local US law enforcement reports increased bulk purchases of poisonous substances such as arsenic.	L	HU (5)	HU (5)	L (0)	10
A-8	New communications are identified between FARC leaders and drug distributors in the United States.	L	U (3)	U (3)	L (0)	6
Scenario B: FARC uses *rompas* to launch mortar attack on USSOUTHCOM headquarters in Miami.						
B-8	An increased number of mortar attacks using *rompas* is reported in Colombia.	HU (6)	HL	C (2)	HU (6)	14
B-4	Known FARC sympathizers are reported purchasing suspicious quantities of liquid petroleum gas canisters.	HU (5)	L	U (3)	U (3)	11
B-3	Hispanic males are observed taking photos of USSOUTHCOM headquarters from a distance.	U (4)	HL	C (2)	C (2)	8
B-6	Recent FARC guerrilla defectors mention a mock-up building in the Amazon is being used for target practice with *rompas*.	U (3)	L	C (1)	U (3)	7
B-7	USSOUTHCOM employees tell their supervisors that they are being approached by strangers and asked who works where in the complex.	U (4)	HL	L (1)	C (2)	7

Table 12.9 ▶ *(Continued)*

Number	Indicator	Scenario A	Scenario B	Scenario C	Scenario D	Score
Scenario C: FARC assassinates Colombian ambassadors with IRA support.						
C-6	Colombians in New York report suspicious persons loitering outside the mission offices.	U (4)	U (4)	HL	U (4)	12
C-7	Suspected FARC members entering the United States are found in possession of Colombian military uniforms.	U (4)	U (4)	HL	U (4)	12
C-1	There are reports of FARC meetings and communications with the IRA.	U (4)	C (2)	HL	U (4)	10
C-3	Kidnappings of field-grade Colombian military officers surge.	U (4)	C (2)	HL	U (4)	10
C-4	There are intelligence reports of IRA hit squads being dispatched to North America.	U (4)	C (2)	HL	U (4)	10
C-5	FARC informants or defectors report that a special squad is being formed for a major operation "up north."	U (3)	L (0)	L	U (3)	6
Scenario D: Marijuana laced with poison kills many in the vicinity of US military bases.						
D-4	DEA chemists report an increase in marijuana laced with arsenic and other toxic substances.	C (2)	U (4)	U (4)	HL	10
D-6	A new theme emerges on Facebook that marijuana consumption may be more dangerous than most suspect.	C (2)	U (4)	U (4)	HL	10
D-8	Informants report that drug users are complaining that the drugs they are purchasing are contaminated.	HL (0)	U (4)	U (4)	HL	8
D-2	Local drug dealers say they are being surveyed by people up their distribution chain asking for details on their user populations.	C (1)	U (3)	U (3)	L	7
D-3	Local health officials report an increase in drug-related deaths among teenagers.	L (0)	U (3)	U (3)	L	6
D-5	Street informants report that their suppliers are talking about making easy money.	L (0)	U (3)	U (3)	L	6
D-1	Street informants report a "buzz" in the Hispanic community that the FARC is planning a special operation in the United States.	C (1)	C (1)	U (3)	L	5

Note: HL = highly likely to appear; L = likely to appear; C = could appear; U = unlikely to appear; HU = highly unlikely to appear.

Step 9: If a large number of indicators for a particular scenario have been eliminated, develop additional—and more diagnostic—indicators for that scenario.

Step 10: Check the diagnostic value of any new indicators by applying the Indicators Validator™ to them as well.

In this illustration, Scenario B has only five indicators remaining, suggesting that at least two more indicators are needed to ensure an adequate number for that scenario. In this instance, two more indicators have been generated and their diagnosticity examined, as shown in Table 12.10.

Analytic Value Added: **Does each scenario have a robust set of highly diagnostic indicators?** Yes, with the addition of two more diagnostic indicators for Scenario B.

Table 12.10 ▶ FARC Attack on the US Homeland: Adding Diagnostic Indicators

Scenario B: FARC uses *rompas* to launch mortar attack on USSOUTHCOM headquarters in Miami.						
B-9	FARC informants report a special unit is being dispatched to Miami.	U (4)	HL	U (4)	C (2)	10
B-10	The Colombian government finds maps of Miami and USSOUTHCOM headquarters in laptops it has captured.	U (4)	HL	C (2)	C (2)	8

Note: HL = highly likely to appear; L = likely to appear; C = could appear; U = unlikely to appear; HU = highly unlikely to appear.

Do these indicator lists provide useful leads for alerting FBI field offices and state and local fusion centers of plausible, potential emerging threats? Yes, the indicators are sufficiently specific to provide operationally useful guidance to field offices or fusion centers.

Are they focused enough to generate specific collection requirements, giving federal, state, local, and tribal officials a more concrete idea of what to look for? Yes, the technique has generated a robust set of concrete indicators that provide effective guidance to the field.

KEY TAKEAWAYS

- When analysts have little data and a mandate to anticipate a potential terrorist attack, often the best approach is to use imagination techniques to generate a large number of possible outcomes. Then pare this list down by identifying the most plausible or attention-deserving options. Over the long run, this is likely to be a much more efficient way to approach problem solving, especially if the key goal is to avoid surprise.
- Analysts should always assess the diagnosticity of their indicators and immediately discard those that fail the test. Failure to do so can give an analyst a false sense of validation. It can also result in tasking collectors to invest valuable resources in acquiring information that in the long run does not aid in analysis or help solve the problem.

NOTES

1. The description of Red Hat Analysis in this case was taken from the first edition of *Structured Analytic Techniques for Intelligence Analysis.* A more robust approach for conducting Red Hat Analysis has subsequently been developed that appears in the second edition of the book but was not used in this case study.

Table 13.2 ▶ Case Snapshot: Understanding Revolutionary Organization 17 November

Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Simple Hypotheses	p. 171	Hypothesis Generation and Testing
What If? Analysis	p. 250	Challenge Analysis
Foresight Quadrant Crunching™	p. 122	Idea Generation

13 Understanding Revolutionary Organization 17 November

Cases in Intelligence Analysis: Structured Analytic Techniques in Action

Instructor Materials

Analysts often deal with ambiguous situations in which information is limited or unconfirmed, as was the case with the investigation of 17 November (17N). In these situations, diagnostic techniques such as Simple Hypotheses can help explore alternative views and hypotheses systematically. Challenge techniques such as What If? Analysis (with the corollary technique of Indicators) helps analysts think through the viability of the analysis and its implications. Imagination techniques such as Foresight Quadrant Crunching™ can help challenge assumptions and explore the implications of specific hypotheses.

TECHNIQUE 1: MULTIPLE HYPOTHESIS GENERATION: SIMPLE HYPOTHESES

Hypothesis Generation is a category of techniques for developing alternative potential explanations for events, trends, or activities. Hypothesis Generation is part of any rigorous analytic process because it helps the analyst avoid common pitfalls such as coming to premature closure or being overly influenced by first impressions. Instead, it helps the analyst think creatively about a range of possibilities. The goal is to develop an exhaustive list of hypotheses that can be scrutinized and tested over time against both existing evidence and new data that may become available in the future.

This case is well suited to Simple Hypotheses, which employs a group process for thinking creatively about a range of possible explanations for 17N's motives and identity. These explanations, in turn, help expand the thinking of investigators who are working to apprehend and counter the group, as well as security officers working to protect US officials in Athens. Engaging a small group helps to generate a large list of possible hypotheses for further investigation. Simple Hypotheses is a method best used by a diverse group that includes expertise from multiple perspectives and stakeholders. This technique includes an exercise in Structured Brainstorming.

In a classroom or workplace setting, this technique can be used by breaking participants into groups to work in separate breakout sessions or by conducting a simpler class- or conference room–based version. For the breakout group–based version, simply assign groups the task below. For the classroom-based version, have participants silently write down possible hypotheses, list those hypotheses on a whiteboard, group the hypotheses, and then refine the hypotheses.

Task 1.

Use Simple Hypotheses to explore all possible explanations for what kind of group 17 November is.

Step 1: Ask each member of the group to write down on separate 3 × 5 cards or sticky notes up to three plausible alternative hypotheses or explanations. Think broadly and creatively, but strive to incorporate the elements of a good hypothesis that is

- Written as a definite statement
- Based on observations and knowledge
- Testable and falsifiable
- Composed of a dependent and an independent variable

Step 2: Collect the cards and display the results. Consolidate the hypotheses to avoid duplication.

A consolidated set of hypotheses might look like Table 13.4.

Step 3: Aggregate the hypotheses into affinity groups and label each group.

Consider multiple ways to display the affinity groups. In this case, the hypotheses may be grouped by the issue of *autonomy*, addressing the question of whether 17N worked alone or in collaboration with other violent groups active in Greece and Europe. Another important consideration is *motive*, and whether 17N was truly a manifestation of radical politics or whether it was also—or instead—a criminal enterprise.

Step 4: Use problem restatement and consideration of the opposite to develop new ideas.

- **Problem Restatement:** Why did it take twenty-seven years to capture the members of 17N?
- **Consideration of the Opposite:** 17N benefitted from official protection. 17N benefitted from the limitations of Greek police and security services. 17N evaded detection because its attacks were so low-tech. All of these ideas have implications about 17N's identity and motive and help expand explanations for what the group might have been. Also consider whether 17N's longevity might be due to its evolutionary nature. Was 17N consistently the same thing for the length of its period of activity? Might its motives, composition, and objectives have changed over time?

Step 5: Update the list of alternative hypotheses.

Problem restatement augments the list of hypotheses by including the possibility of government collusion or protection. It also raises the possibility that the group's motive, objectives, and identity evolved over time.

Step 6: Clarify each hypothesis by asking Who? What? How? When? Where? and Why?

Table 13.4 ▶ Simple Hypotheses Generation: Examples of Consolidated 17N Hypotheses

• 17N started out as a far-left Greek terrorist group and then became a criminal enterprise.
• 17N was always a criminal enterprise masquerading as a terrorist group.
• 17N was part of a larger pan-European violent extremist movement.

Make a list of each of the categories. Step back and consider how each list could be augmented. "Who" and "What" suggest possible identities: an autonomous group of Greek violent extremists, a criminal enterprise, or a subgroup of a larger regional violent extremist movement? "When" addresses the issue of whether 17N had a consistent identity, composition, and objectives over the years, or whether it evolved. "Where" addresses the theater of operations: All claimed attacks were in Athens, but could there have been activity elsewhere not credited to the group? "How" addresses the longevity of the group's success. If it evaded detection for so many years because of the low-tech nature of its attacks, what does that also say about what it was? "Why" addresses motive: to inspire political revolution, to make money, to advance political goals of invested officials? Refine this list to make the categories as mutually exclusive as possible. This helps clarify the hypotheses.

Step 7: Select the most promising hypotheses for further exploration.

- 17N is a Greek violent far-left group that, for a period of time, worked in collaboration with other violent groups, Greek and/or foreign, to inspire a Marxist revolution.
- 17N is a Greek violent extremist group working in conjunction with criminal enterprises, in Greece and regionally, both for monetary gain and to advance a political agenda.
- 17N is a group manipulated by or influenced by Greek political officials to engage in dirty politics in Athens.

Analytic Value Added: Did using the technique help you challenge conventional wisdom about the group and its motives? The technique generated several new ways to think about the group, suggesting different motives in particular. This is important because the analyst now will be looking for additional indicators that can prove or disprove each of the hypotheses.

Did it reveal ideas or concepts that you might have missed if you had engaged in conventional brainstorming only? The technique raised the possibility that 17N might be operating entirely or partially for criminal motives and may have evolved over time—ideas that certainly would require more research.

Was it difficult to select those hypotheses that deserved the most attention? As themes emerged from the Structured Brainstorming process, it was helpful to use

them to develop an expanded set of hypotheses that reflected the themes. Selecting the most important hypotheses is easier if the analysts work from a specific set of criteria that defines what makes a good hypothesis.

TECHNIQUE 2: WHAT IF? ANALYSIS

What If? Analysis posits that an event has occurred with the potential for a major positive or negative impact and then explains how it came about. This technique is best used when analysts are having difficulty getting others to focus on the potential for, or the consequences of, a high-impact/low-probability event to occur. It is also appropriate when a controversial mindset is well ingrained. In the late 1990s, US security officials continued to be concerned about the potential for an attack by the group. Because What If? Analysis shifts the focus from whether an event could occur to how it might happen, the technique allows analysts to make more informed judgments about whether such developments—even if unlikely—might actually occur.

Task 2.

Assume you are an analyst working at the US Embassy in Athens in 1999. Use What If? Analysis to explore the viability and likely nature of another attack on a US official in Athens by 17N. It had been eight years since 17N had killed a US official. The rocket shot at the US Embassy's back gate in 1996 spoke to intent, but also to limited capabilities. Security at the US Embassy in Athens was at an all-time high. Not only did senior officers at the embassy have armored vehicles and robust protection, but they, and all embassy staff, were advised to vary their routes and lower their profiles. What if 17N had managed to kill a US official despite this high security? What would it look like? What would it suggest?

Step 1: Begin by assuming what could happen has actually occurred. In December 1999, 17N has attacked yet another US official in Athens despite enhanced security.

Step 2: Develop a chain of argumentation—based on evidence and logic—to explain how this event could have come about. Create more than one scenario or chain of argument. In Figure 13.1 we have described how one of these scenarios might be portrayed.

- Scenario A: 17N shoots US military officer
- Scenario B: 17N bombs US Embassy vehicle in Athens
- Scenario C: 17N assassinates US political counselor as he leaves for work

Step 3: Generate a list of indicators for each scenario that would point to the events starting to play out. A sample set of indicators is provided in Table 13.5.

Step 4: Assess the level of damage or disruption that would result from each scenario and how difficult it would be to overcome.

Figure 13.1 ▶ What If? Analysis Scenario: 17N Shoots US Military Officer

It is 1999, the peak of the NATO campaign in the Balkans. The majority of Greeks feel a religio-ethnic affinity with the Serbs, and vehemently oppose the strikes and any overt support given to the Bosnians and Kosovars by the West. Popular protests make it clear that this is an issue that resonates with a large swath of the Greek people. 17N sees an opportunity to advance its agenda and decides to target a US military officer with NATO ties. Senior US military officers or defense attachés affiliated with the embassy and stationed in Athens are afforded careful security protection by both DoD and Diplomatic Security. They have armored vehicles and, sometimes, security escorts, and their drivers carefully vary their routes. All vehicles entering the embassy compound are screened for explosives, and the building itself is inaccessible to outsiders. Their residences and families are similarly protected. Lower-level officers also receive security training and are instructed to report any signs of surveillance or unusual behavior. All local embassy hires are carefully screened.

Despite this high security, 17N is still focused on targeting an American military officer and making a statement about what the group perceives to be immorality of a US-backed NATO campaign. It decides to monitor the major restaurants and tourist venues in central Athens, where American Embassy personnel are known to congregate, but finds that there are too many people and it is too hard to distinguish which Americans might have military affiliations. It surveils all cars coming and going from the embassy compound and finds that some lower-level officers with less security detail are not always careful about varying their commutes to and from work, especially after several months at post.

One young man in particular, who drives an old model Honda, takes the same major thoroughfare to the embassy from his residence every day. His short haircut suggests he might have a military affiliation. 17N decides it is their best shot and plots a drive-by shooting timed for the peak morning rush hour. It prepares the proclamation in advance, accusing the nameless American of being centrally involved in the "incursion into Serbian sovereign space."

Table 13.5 ▶ What If? Analysis: Indicators of Military Officer Scenario Starting to Unfold

- Possible surveillance activity reported by embassy security personnel guarding the embassy compound gates
- Reports of unidentified or suspicious vehicles being parked in vicinity of embassy residences
- 17N posts statements describing US military involvement in Bosnia as inhumane and politically biased
- Greek police inform the embassy that they have picked up a "buzz" on the streets that a terrorist attack is being planned
- Proactive embassy security personnel surveil traditional 17N ambush sites and observe suspicious activity by two men who may be casing the site

For the military officer scenario, the killing would signal that 17N was still active, and security would be heightened not only for US officials but also other for diplomatic posts in Athens and the Greek government and private sector.

Step 5: Rank the scenarios in terms of which deserves the most attention by taking into consideration the difficulty of implementation and the potential severity of the impact.

Depending on how the other scenarios are constructed, a likely ranking in descending order of difficulty of implementation would be:

- Scenario C: 17N assassinates US political counselor near US Embassy
- Scenario A: 17N shoots US military officer en route to work
- Scenario B: 17N bombs US Embassy vehicle in Athens

Analytic Value Added: Did the technique help you generate new ways of thinking about the problem? The technique moved the conversation beyond the debate over whether 17N is still a viable terrorist organization, but it did not generate new ideas regarding what type of attack might be launched. It did, however, provide insight into the likelihood of a particular type of attack based on degree of difficulty.

Did it help you assess how difficult each scenario would be to carry out? By working one's way step by step through each scenario, it is easier to assess how 17N is most likely to launch each attack and assess what is required for each to succeed.

Did the exercise indicate that any new security measures should be implemented? By describing in some detail how an attack would be launched—working from the planning stages to the actual attack—it made it easier to anticipate what types of security measures would be needed to forewarn officials that planning for such an attack may be underway. Generating indicators for a scenario can be a daunting task, particularly when so little is known about the group or its key members—but the process helps stimulate a useful list of things that might be observed and reported.

TECHNIQUE 3: FORESIGHT QUADRANT CRUNCHING™

Quadrant Crunching™ combines the methodology of a Key Assumptions Check with Multiple Scenarios Generation to generate an array of alternative scenarios or stories. Two versions of Quadrant Crunching™ have evolved in recent years; each technique serves a different analytic function:

In **Classic Quadrant Crunching™**, the analyst begins with a lead hypothesis (an example of a lead hypothesis would be, "A criminal group has penetrated a large corporate database to steal Personal Identity Information [PII]"), breaks the lead hypothesis into its component parts (*criminal group/steal PII*); flips the assumption inherent in each segment (*noncriminal group/alternative motive*); and brainstorms contrary dimensions or explanations (usually one to three) consistent with each flipped assumption (*business competitor or foreign country, to download corporate data or to alter corporate information*). The analyst then arrays the contrary dimensions or explanations in a 2 × 2 matrix, generating new and unique attack scenarios in each quadrant (*Business competitor penetrates database to download corporate data, Business competitor penetrates database to alter corporate information, Foreign country penetrates database to download corporate data,* and *Foreign country penetrates database to alter information.*) As more dimensions of the problem are considered, the number of potential scenarios increases rapidly and the chances of being surprised by a new and unanticipated development diminish.

Classic Quadrant Crunching™ differs from multiple scenarios analysis in two ways: (1) the focus is on ways things could happen other than what is generally expected, and (2) the technique relies on contrary dimensions versus spectrums to define the endpoints of the *x*- and *y*-axes.

The **Foresight Quadrant Crunching™** technique differs from Classic Quadrant Crunching™ in that the focus is on *all* of the ways something could happen, not just what might be different. In this version of the technique, the lead hypothesis dimensions are included in the analysis. Foresight Quadrant Crunching™ is similar to Classic Quadrant Crunching™, however, in that both use contrary dimensions versus spectrums to define the endpoints of the *x*- and *y*-axes.

To use our previous example again, the analyst begins with a lead hypothesis (A criminal group has penetrated a large corporate database to steal Personal Identity Information [PII]), breaks the lead hypothesis into its component parts *(criminal group/to steal PII)*; flips the assumption inherent in each segment *(noncriminal group/alternative motives)*; brainstorms contrary dimensions (usually from one to three) consistent with the flipped assumption *(business competitor* or *foreign country, to download corporate data* or *to alter corporate information)*; and then lists all possible combinations, comprising nine different attack scenarios:

1. Criminal group penetrates database to steal PII.
2. Criminal group penetrates database to download corporate data.
3. Criminal group penetrates database to alter corporate information.
4. Business competitor penetrates database to steal PII.
5. Business competitor penetrates database to download corporate data.
6. Business competitor penetrates database to alter corporate information.
7. Foreign government penetrates database to steal PII.
8. Foreign government penetrates database to download corporate data.
9. Foreign government penetrates database to alter corporate information.

The Foresight Quadrant Crunching™ technique is particularly applicable to the 17N case because (1) little was known about the identity of the group members or their plans while they were active, and (2) in several cases only one credible alternative dimension merited the analysts' attention. Foresight Quadrant Crunching™ helps the analyst identify and challenge key assumptions that may underpin the analysis while generating a comprehensive and mutually exclusive array of credible scenarios to help investigators focus on the most likely types of attacks to anticipate.

Task 3.

It is now 2001, and you are an analyst based in the US Embassy in Athens, supporting the ongoing investigation of 17N. The embassy is beginning to focus its attention on preparing for the Olympic Games in Greece in 2004. Use Foresight Quadrant Crunching™ to brainstorm all possible ways 17N might pose a serious threat to the American community.

Step 1: State your lead hypothesis.

This hypothesis should reflect either the analytic consensus regarding the most likely means of attack or the current conventional wisdom, which usually reflects how such attacks have been launched in the past. 17N's attacks against American targets traditionally were assassinations of US government or military officials using a signature 17N handgun. For this exercise, we will use the following as our lead hypothesis: a 17 November operative will shoot a US official in Athens prior to the Olympic Games in 2004.

Step 2: Break the lead hypothesis down into its component parts based on the journalist's list of Who? What? How? When? Where? and Why?

Step 3: Identify which of these components are most critical to the analysis.

Step 4: For each of the critical components, identify either one or three contrary dimensions in a table, as shown in Table 13.6.

Six key components were identified in this exercise—one for each of the "five W's and H" questions. Three of the key components (not shaded in Table 13. 6) deserve serious discussion and analysis because the contrary dimensions could pose significant new challenges for how best to protect US officials from a 17N attack before and during the 2004 Olympics.

- **Who?** Historically, 17N has only targeted individuals deemed guilty of "crimes" against the Greek people or nation: US, Greek, European, and Turkish military

Table 13.6 ▶ Foresight Quadrant Crunching™: Contrary Dimensions

Key Assumptions	Lead Hypothesis	Contrary Dimension	
Who? (target)	US official	Tourists attending the Olympics	
What? (tactics)	Assassination	Hostage taking or kidnapping	
How? (weapon)	Shooting with signature weapon	Remote-control bomb	Rockets
When? (timing)	Before the August 2004 Olympics	During an Olympic event	
Where? (location)	In metropolitan Athens	Outside Athens (including other Olympic venues)	
Why? (motives)	To advance extreme political ideology	Protest holding the Olympics in Greece	Protest Greek ties to the United States

officers and diplomats, as well as members of the Greek wealthy elite. With the scheduling of the Olympics in Greece, however, 17N might decide to change tactics and target those attending the Olympics in order to gain more publicity for its movement. 17N might also conclude that it would be more likely to succeed if it shifted to new tactics that would require a different type of security mitigation strategy than what had been previously practiced by the police.

- **What?** 17N has operated with different modi operandi over the years. The nature of 17N attacks has evolved over time, increasing in sophistication and daring, from shootings on abandoned streets late at night to makeshift rockets launched on busy intersections in downtown Athens in broad daylight. There is no reason not to explore the possibility that its tactics may continue to change, advancing to kidnappings or hostage taking, especially if the group sees an Olympics attack as helping them gain international publicity.
- **Where?** The 2004 Olympics involves venues across Greece; 17N could conclude that sites outside Athens could be more vulnerable targets. Although 17N would be launching an attack outside of its historical comfort zone—greater metropolitan Athens—it might conclude that the benefits outweighed the risks.

The remaining questions are poorer candidates for a Foresight Quadrant Crunching™ exercise because (1) the alternatives to the lead hypothesis are not likely to have significant impact on how the analysis is conducted, or (2) the alternatives would not require different security strategies to mitigate the threat.

- **How?** The primary concern is whether a lethal attack might occur, not the type of weapon that would be used to kill people. 17N only carried out three types of attacks during its twenty-seven years of activity: shootings with its signature handguns, bombings, and rocket attacks. This speaks both to the group's *capabilities* and to its *intent*. 17N focused on targeting select individuals, not on carrying out attacks that resulted in mass casualties. The group learned over time that its makeshift rockets were often hard to manipulate and control. In one instance, a rocket missed its target (Vardinoyiannis 1990), and in another, it inadvertently killed an innocent bystander (Paliokrassas 1992). This would suggest that the group is unlikely to use this tactic again.
- **When?** This is important, but whether an attack would be launched before or during the Olympics would have little impact on how the analysis is conducted, although it may have larger implications for those charged with managing the crowds. The exercise raises a good question, however: Would 17N's avoidance of injuring "innocent civilians" affect its choice of timing?
- **Why?** This question explores multiple motives for launching an attack. Whether 17N attacked to advance an extremist ideology, to protest Greece's participation in or hosting of the Olympic Games, or to protest Greece's close ties with the United States more generically, it would probably not change the nature of the attack.

Step 5: Array combinations of these contrary assumptions in sets of 2 × 2 matrices.

For this exercise, 2 x 2 matrices will be constructed based on both the lead assumption and selected contrary dimensions.

- **Who? (target):** US officials or tourists attending the Olympics
- **What? (tactics):** Assassination or hostage taking/kidnapping
- **Where? (location)**: In metropolitan Athens or outside Athens (including other Olympic Games events)

These pairs of dimensions then must be paired to create three different matrices with a total of twelve combinations. For ease of discussion, each quadrant has been given a number identifier. For example, in the first matrix, Quadrant 1 refers to an attack scenario involving an attack on a US Embassy official in Athens. The twelve possible combinations are shown in Table 13.7.

Step 6: Generate one or two credible scenarios for each quadrant.

For each cell in each matrix, generate one or two examples of how this scenario could play out. In some quadrants, the most likely scenario might be relatively easy to identify. For example, the scenarios generated for Quadrants 1 and 5 would look like traditional 17N attacks. The terrorists probably would stay within their comfort zone, selecting an embassy official with an established pattern who would offer an easy target in Athens—a city whose chaos and crowds afford a certain level of camouflage for the operatives.

The scenario for Quadrant 10 would require 17N to carry out a shooting outside of downtown Athens, its usual domain. Staging an attack in a less-populated location such as Olympia or Marathon, where some of the Olympics events will be held, might mean that the drivers would opt for the motorcycle approach, and limit their exposure before the attack. The scenario for Quadrant 11 and would require consideration of the risk of hurting innocent bystanders, something 17N had avoided in the past.

In other quadrants, it could prove difficult to come up with a credible scenario, but generating scenarios for all the quadrants will usually stretch the analysts' thinking, forcing them to reframe the problem in a variety of ways. In so doing, they are almost certain to gain new insights and come up with a more creative set of potential attack scenarios.

Table 13.7 ▶ Foresight Quadrant Crunching™: Potential Attack Scenarios

Target/Location			
1	US official	3	US official
	In metropolitan Athens		Outside Athens
2	Tourists at Olympics	4	Tourists at Olympics
	In metropolitan Athens		Outside Athens
Target/Tactics			
5	US official	7	US official
	Assassination		Hostage taking/kidnapping
6	Tourists at Olympics	8	Tourists at Olympics
	Assassination		Hostage taking/kidnapping
Location/Tactics			
9	In metropolitan Athens	11	In metropolitan Athens
	Assassination		Hostage taking/kidnapping
10	Outside Athens	12	Outside Athens
	Assassination		Hostage taking/kidnapping

Step 7: Arrange all the scenarios generated in a single list with the most credible scenario at the top of the list and the least credible at the bottom using preestablished criteria.

In this example, possible criteria might include those scenarios that are targeting lower-level officers with less security protection or multiple attacks designed to heighten the perception of the group's capabilities. After establishing a solid set of criteria, rate each scenario on a 1 to 5 scale, with 5 indicating the scenario that is highly deserving of attention and 1 indicating that officials should give this scenario a relatively low priority. Place the scenario deserving the most attention at the top of the list, and the least credible scenario at the bottom.

If a scenario makes little sense or is highly unlikely, place an "x" in the box and eliminate it from further consideration. For example, a scenario involving a hostage taking outside Athens during the Olympic Games (Quadrant 12) would be well outside the scope of 17N's practice, difficult to organize, and probably could be dropped from the list.

Once the unlikely scenarios are dropped, the next task is to prioritize the remaining scenarios. A useful template is provided in Table 13.8. Different analysts might rate each scenario depending on its vantage point. For example, were they primarily concerned about security for the Olympic Games or the security of the embassy staff? Had they worked on previous cases involving the taking of hostages and believed this was a viable threat too often discounted by other analysts?

Table 13.8 ▶ Foresight Quadrant Crunching™: Rating the Attack Scenarios

Quadrant	Alternative Scenario	Rating
5	US official assassinated in Athens en route to Olympic event	5
9	US official visiting Games assassinated as he leaves hotel	5
3	US official shot when attending Olympic event in Marathon	4
1	Car with US official sprayed with bullets on Athens street	3
6	Several US tourists assassinated at Olympics site by sniper	2
2	Bus taking US tourists from hotel to Athens Olympic event bombed	2
10	US tourist bus en route to Olympic event outside Athens bombed	2
7	Visiting US official taken hostage en route to Olympic event	2
4	Bus taking Americans to Olympic event outside Athens bombed	2
11	Americans at Athens hotel taken hostage and rooms set afire	1
8	Americans dining at an Olympic site restaurant held hostage	X
12	Americans staying at hotel outside Athens taken hostage	X

Analytic Value Added: Which scenario is the most deserving of attention? The terrorists have shown a consistent pattern of conducting well-planned, focused attacks on US government or military officials while avoiding the killing of innocent civilians. They also are more practiced at operating in metropolitan Athens and probably would continue to prefer that area of operations.

Should attention focus on just one scenario, or could several scenarios play out simultaneously? It probably would be wise to give serious consideration to all scenarios receiving a rating of three or above. Although 17N's pattern of behavior has been fairly consistent over time, new factors could always come into play, such as the emergence of a new leader or a faction that advocates expanding beyond its traditional patterns.

Are any key themes present when reviewing the most likely set of attention-deserving scenarios? The most likely themes are the likelihood that 17N will continue to use small arms or bombs and seek to avoid killing innocent people, but may expand its theatre of operations.

Does this technique help you determine where to devote the most attention in trying to deter an attack? The technique helps the analyst consider a larger range of attacks and to develop specific criteria for which attacks are most likely to occur. By forcing analysts to think operationally in terms of how easy or difficult it would be to launch various attacks, the analysts get a better sense of what is most feasible, and therefore more likely to occur.

Does it help you challenge any key assumptions regarding how an attack might take place? The technique helped challenge several assumptions. For example, an attack might not necessarily have to take place in Athens. It is possible that some members of the group might be just as familiar with the city landscape of a surrounding town that was also going to play host to some Olympic events. Such a location might also be more attractive as a setting for an attack if it had less police scrutiny.

CONCLUSION

On June 29, 2002, a botched attempted bombing by one of the core members of 17N led to his arrest, confession, and the subsequent unraveling of the group. Savvas Xiros, a name new to Greek police, was seriously injured when a homemade explosive device he had placed behind a Flying Dolphin ferry ticket kiosk in Piraeus exploded prematurely. Xiros, a largely self-taught bomb maker, lost several fingers and suffered permanent damage to his eyes. The port police who responded to the blast discovered a second bomb and, more significantly, a bag containing a gun that linked to a 17N bank robbery in 1984 in which a police officer had been killed.[1] After Savvas's photo was placed on Greek television, an anonymous caller provided information connecting him to a safehouse.[2] Two apartments were discovered, chock full of all the materials 17N used to carry out its attacks: stolen license plates, keys, forging materials, pvc pipes, guns, bullets, costumes, proclamations, surveillance notes, and perhaps most interesting of all, a detailed ledger that chronicled the members' pay and expenses per operative alias.[3]

Savvas awoke in the hospital under heavy police guard, and spent the next few weeks being interrogated. Police aggressively pursued all leads stemming from Savvas's

confession and the safehouses and within days had arrested three of his brothers, all sons of a Greek Orthodox priest from a small village in Northern Greece. By mid-July, another eight operatives had been identified and arrested.

Savvas Xiros's cohorts included a real estate agent, a schoolteacher, a shopkeeper, a telephone operator, and a musician, many connected through familial and village ties. He himself was an icon painter by trade.[4] The group's operational leader and account keeper, Dimitris Koufondinas, managed to hide for several weeks on a nude beach on one of the Greek islands but eventually turned himself in. Taking a taxi to police headquarters in Athens, he identified himself to the police officer on duty as the most wanted man in Greece.[5] He and his partner had eked out a living as beekeepers.

Missing from this cadre, however, was the ideological leadership. The investigation led police to Lipsi, a remote Dodecanese island where Alexandros Giotopoulos, a French-educated radical and former head of the Junta resistance group LEA (Popular Revolutionary Resistance), lived under an assumed name, Mihalis Economou. Giotopoulos's father had been a well-known Trotskyite,[6] and Giotopoulos and his French wife lived in a pink house on Lipsi, where he often held court at the local tavern on politics and tussled with local authorities over his right to violate the regulations for whitewashing his home. Authorities from Athens arrived in Lipsi just in time to arrest Giotopoulos as he was waiting to catch the next ferry to Turkey. The earliest crimes of 17N were never tried in court due to a twenty-year statute of limitation on murder in Greece, and Giotopoulos never admitted to any involvement[7], but he is largely believed to have been the man who shot and killed Richard Welch in 1975.

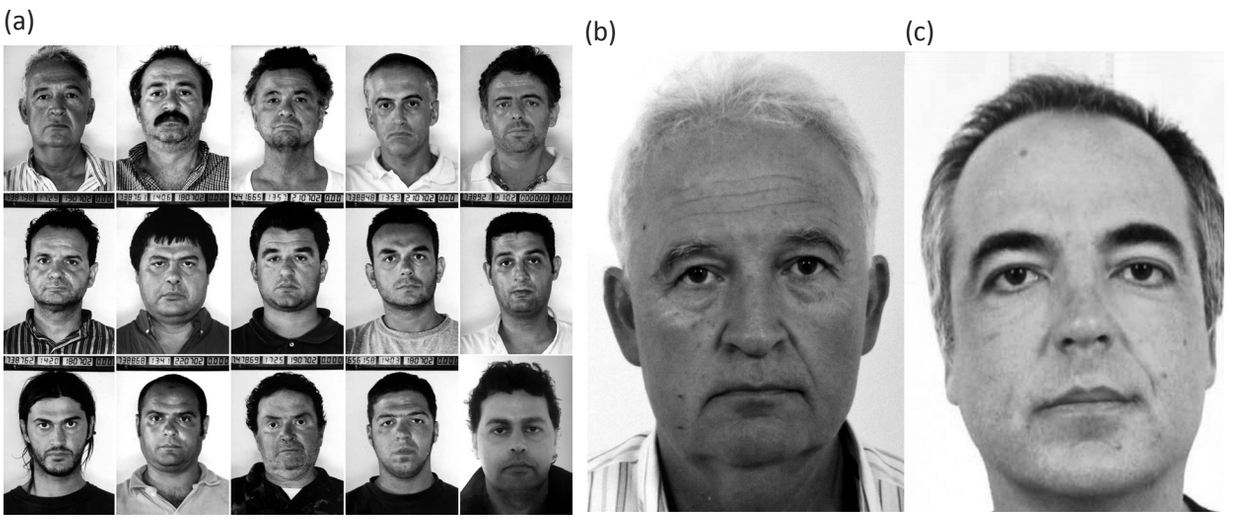
The unmasked members of what had become the great Greek unsolved mystery revealed themselves to be a parochial assortment of men, but for almost three decades, the unidentified members of 17N had assumed an almost mythical role in Greek society. What was revealed was an autonomous and indigenous violent far-left group, whose time was finally over.

KEY TAKEAWAYS

- When information is limited or ambiguous, it is helpful to explore alternative explanations for what appears to be or what might be to help find overlooked explanations and investigative leads.
- Multiple Hypotheses Generation helps develop more nuanced explanations, such as the possibility that a group may have changed or evolved over time.

Figure 13.2 ▶ Mug Shots of the 17N Suspects

The suspects were apprehended in the summer of 2002. Far right is the operational mastermind, Koufondinas, and to his left is the ideological leader, Giotopoulos.



SOURCE: (a) AP Photo/File. (b) AP Photo/HO/Greek Police. (c) AP Photo/File.

- Using techniques such as Foresight Quadrant Crunching™, analysts can better anticipate the unanticipated and create alternative stories or "bins" that could prove useful when newly obtained information does not fit comfortably within established investigative categories.
- The What If? Analysis technique is useful for refocusing attention operationally on potential threats and vulnerabilities, and assessing their likelihood.
- All three techniques allow for a more rigorous and nuanced assessment of the group's capability and intent, allowing analysts to leapfrog to a new level of understanding.

NOTES

1. Tamara Makarenko and Daphne Biliouri. "Is this the end of 17N?" *Jane's Intelligence Review* 14 (2002): 9.
2. Ibid.
3. Kiesling, Brady, *Greek Urban Warriors: Resistance and Terrorism 1967–2012*, Athens: Lycabettus Press (forthcoming).
4. Shawn Choy, "In the Spotlight" Revolutionary Organization 17 November," CDI Terrorism Project, August 5, 2002. www.cdi.org/terrorism/17N-pr.cfm
5. George Kassimeris, "Fighting for Revolution? The life and death of Greece's revolutionary organization 17 November, 1975–2002" *Journal of Southern Europe and the Balkans* (6) 2004: 259.
6. Choy, CDI Terrorism Project.
7. Kassimeris, "Fighting for Revolution?" 270-272.

Table 14.2 ▶ Case Snapshot: Defending Mumbai from Terrorist Attack

Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Structured Brainstorming	p. 102	Idea Generation
Red Hat Analysis	p. 223	Assessment of Cause and Effect
Classic Quadrant Crunching™	p. 122	Idea Generation
Indicators	p. 149	Scenarios and Indicators
Indicators Validator™	p. 157	Scenarios and Indicators

14 Defending Mumbai from Terrorist Attack
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

It is mid-October 2008. You are an analyst working in the Mumbai Police Department, and you just received the US warning about the threat to Mumbai from the Intelligence Bureau in New Delhi. Analysis of the threat has to be done quickly in order to develop guidance to help authorities anticipate and detect the type of attack that is being planned. Although no analyst has a crystal ball, it is incumbent upon analysts to help law enforcement officials and policy makers anticipate how adversaries will behave, outline the range of possible futures that could develop, and recognize the signs that a particular future is beginning to take shape. The techniques in this case—Structured Brainstorming, Red Hat Analysis, Classic Quadrant Crunching™, Indicators, and the Indicators Validator™—can help analysts tackle each part of this task.

The challenge for law enforcement analysts in this case is to forecast how the anticipated attack is most likely to be launched and, in so doing, help local officials and businesspeople prevent or mitigate the damage of such an attack. When confronted with this challenge, the first reaction of many students is to propose that the Indian government increase its vigilance, issue an alert to local officials that a terrorist attack on Mumbai is imminent, and ask them to look out for any suspicious activity that would indicate that such an attack is being planned or is underway. Unfortunately, such guidance lacks sufficient specificity to be of much value to Mumbai law enforcement officials and businesspeople. The purpose of these exercises is to show that with the use of structured analytic techniques, analysts can generate a plausible set of attention-deserving scenarios and create tailored lists of collection requirements that provide operational value to local officials and businesspeople.

These instructor materials are built around what actually occurred, but a successful student analysis need not mirror the events on the day of the attack. Instead, instructors and the students should judge the resulting analyses on the basis of how well the students apply the analytic process and the extent to which they identify well-considered and actionable steps that intelligence operators, law enforcement officials, and collection agencies can use to counter the threat.

TECHNIQUE 1: STRUCTURED BRAINSTORMING

Brainstorming is a group process that follows specific rules and procedures designed for generating new ideas and concepts. The stimulus for creativity comes from two or more analysts bouncing ideas off each other. A brainstorming session usually exposes an analyst to a greater range of ideas and perspectives than the analyst could generate alone, and this broadening of views typically results in a better analytic product. (See eight rules for successful brainstorming in Box 14.2.)

Structured Brainstorming is a more systematic twelve-step process for conducting group brainstorming. It requires a facilitator, in part because participants are not allowed to talk during the brainstorming session. Structured Brainstorming is most often used to identify key drivers or all the forces and factors that may come into play in a given situation.

Task 1.

Conduct a Structured Brainstorming exercise to identify all the various modes of transport the assailants might use to enter Mumbai.

Box 14.2 EIGHT RULES FOR SUCCESSFUL BRAINSTORMING

1. Be specific about the purpose and the topic of the brainstorming session.
2. Never criticize an idea, no matter how weird, unconventional, or improbable it might sound. Instead, try to figure out how the idea might be applied to the task at hand.
3. Allow only one conversation at a time and ensure that everyone has an opportunity to speak.
4. Allocate enough time to complete the brainstorming session.
5. Engage all participants in the discussion; sometimes this might require "silent brainstorming" techniques such as asking everyone to be quiet for five minutes and write down their key ideas on 3 × 5 cards and then discussing what everyone wrote down on their cards.
6. Try to include one or more "outsiders" in the group to avoid groupthink and stimulate divergent thinking. Recruit astute thinkers who do not share the same body of knowledge or perspective as other group members but have some familiarity with the topic.
7. Write it down! Track the discussion by using a whiteboard, an easel, or sticky notes.
8. Summarize key findings at the end of the session. Ask the participants to write down their key takeaways or the most important things they learned on 3 × 5 cards as they depart the session. Then, prepare a short summary and distribute the list to the participants (who may add items to the list) and to others interested in the topic (including those who could not attend).

Step 1: Gather a group of analysts with knowledge of the target and its operating culture and environment.

Step 2: Pass out sticky notes and marker-type pens to all participants. Inform the team that there is no talking during the sticky-notes portion of the brainstorming exercise.

Step 3: Present the team with the following question: What are all the various modes of transport the assailants might use to enter Mumbai?

Step 4: Ask them to pretend they are Muslim terrorists and simulate how they would expect the assailants to think about the problem. Emphasize the need to avoid mirror imaging. The question is not "What would you do if you were in their shoes?" but "How would the assailants think about this problem?"

Step 5: Ask the group to write down responses to the question with a few key words that will fit on a sticky note. After a response is written down, the participant gives it to the facilitator, who then reads it out loud. Marker-type pens are used so that people can easily see what is written on the sticky notes when they are posted on the wall.

Step 6: Post all the sticky notes on a wall in the order in which they are called out. Treat all ideas the same. Encourage participants to build on one another's ideas. Usually an initial spurt of ideas is followed by pauses as participants contemplate the question. After five or ten minutes there is often a long pause of a minute or so. This slowing down suggests that the group has "emptied the barrel of the obvious" and is now on the verge of coming up with some fresh insights and ideas. Do not talk during this pause, even if the silence is uncomfortable.

Step 7: After two or three long pauses, conclude this divergent-thinking phase of the brainstorming session.

Step 8: Ask all participants (or a small group) to go up to the wall and rearrange the sticky notes by affinity groups (groups that have some common characteristics). Some sticky notes may be moved several times; some may also be copied if an idea applies to more than one affinity group.

Step 9: When all sticky notes have been arranged, ask the group to select a word or phrase that best describes each grouping.

Step 10: Look for sticky notes that do not fit neatly into any of the groups. Consider whether such an outlier is useless noise or the germ of an idea that deserves further attention.

Step 11: Assess what the group has accomplished. How many different ways have you identified that the assailants could transport a team to Mumbai?

Step 12: Present the results, describing the key themes or dimensions of the problem that were identified. Consider less conventional means of presenting the results by engaging in a hypothetical conversation in which terrorist leaders discuss the issue in the first person.

Over the course of the exercise, students should generate between twenty and fifty ideas. Groups familiar with the region or with terrorist activity are likely to generate more ideas. The most obvious ways to group the responses would be to distinguish efforts to access Mumbai by sea, by land, or by air. If the students are having trouble coming up with ideas or their ideas are too general, ask them to drill down on specific ways the terrorists would come to Mumbai using different modes of transport. Table 14.4 provides a sampling of likely responses. Encourage the students to be creative, as this usually builds energy within the group. Some groups, for example, have proposed using gliders, parachutes, and even Segways. Other seemingly out-of-the-box ideas that could merit attention are bicycle tours and the use of human-trafficking networks.

Analytic Value Added: Were we careful to avoid mirror imaging when we put ourselves "in the shoes" of Muslim terrorist planners? While a regular citizen might use commercial air or a border crossing to enter India, we cannot assume that terrorists would do the same. The risks of apprehension are too high. Also, some of the ideas generated may not prove practical if the terrorists need to transport weapons and explosives with them to Mumbai. Crossing the border or transiting through an airport might prove impractical, suggesting that ideas such as using commercial aircraft for transit are unlikely.

Did we explore all the possible forces and factors that could influence how the terrorists might gain access to Mumbai to launch their attack? The list appears to be comprehensive, covering all potential forms of transit.

Did we cluster the ideas into coherent affinity groups? The ideas easily fell into three categories: land, sea, and air. A key consideration was whether the same mode of transport would be used for the entire transit or a two-stage process would be more effective, particularly if the assailants come by sea from Pakistan. Other groupings that one could consider would be based on how the form of transit was acquired, for example, by purchase, rental, hijacking, or buying tickets.

How did we treat outliers or sticky notes that seemed to belong in a group all by themselves? Did the outliers spark any new lines of inquiry? The brainstorming exercise should generate several outliers, such as the use of a tourist helicopter to launch an attack or the use of taxis. Another outlier to consider would be for the terrorists to hide themselves and their supplies in a large cargo container on a plane or a ship and sneak out before passing through customs inspection or bribe the customs inspector to look the other way. The use of submersibles similar to those used to smuggle drugs from Colombia to the United States would be a creative, albeit potentially more expensive, solution. The exercise might also prompt students to consider the use of "insiders," such as residents of Mumbai who have agreed to provide their vehicles for a price or out of sympathy for the movement's objectives.

Table 14.4 ▶ Modes of Transit into Mumbai: Brainstormed Examples

By Sea	By Land	By Air
If departing from Pakistan:	Drive personal vehicles.	Fly commercial air from Pakistan.
Take large boat to Mumbai.	Drive commercial truck.	Fly commercial air from India.
Hide in large container ship.	Rent large truck.	Fly private aircraft from Pakistan.
Take public ferry.	Take train to Mumbai.	Fly private aircraft from India.
If two-staged transit:	Take bus to Mumbai.	Hijack small airplane.
Take large boat to submersible.	**If two-staged transit:**	Hide in large cargo container in cargo plane.
Take large boat to coast near Mumbai and transfer to Zodiacs.	Drive large commercial truck and hijack taxis or bus on outskirts of city.	**If two-staged transit:**
Take large boat to coast near Mumbai and transfer to truck, cars, or taxis.	Take train and hijack bus or taxis at train station.	Fly private aircraft to vicinity of Mumbai and rent or hijack helicopter to enter city.

TECHNIQUE 2: RED HAT ANALYSIS

Analysts frequently endeavor to forecast the actions of an adversary or a competitor. In doing so, they need to avoid the common error of mirror imaging, the natural tendency to assume that others think and perceive the world in the same way as they do. Red Hat Analysis is a useful technique for trying to perceive threats and opportunities as others see them, but this technique alone is of limited value without significant understanding of the cultures of other countries, groups, or people involved. There is a great deal of truth to the maxim that "where you stand depends on where you sit." By imagining the situation as the target perceives it, an analyst can gain a different and usually more accurate perspective on a problem or issue.

Reframing the problem typically changes the analyst's perspective from that of an analyst observing and forecasting an adversary's behavior to that of someone who must make difficult decisions within that operational culture. This reframing process often introduces new and different stimuli that might not have been factored into a traditional analysis.

Task 2.

Use Red Hat Analysis to prioritize the list of various modes of transport the terrorists might use to enter Mumbai.[1]

Step 1: Gather a group of experts with in-depth knowledge of the target, operating environment, and the terrorist group's motives and style of thinking. If at all possible, try to include people who are well grounded in Mumbai's culture, speak the language, share the same ethnic background, or have lived extensively in the region.

Step 2: Ask group members to develop a list of criteria that they would most likely use when deciding which modes of transport they personally would choose to enter Mumbai. The reason for first asking the group *how* it would act is to establish a baseline for assessing whether the terrorists are likely to act differently.

Key criteria would include the following:

- Minimizing the chances of detection prior to implementing the plan.
- Minimizing the chances of detection while in transit.
- Minimizing the chances of detection during the attack.
- Providing adequate means to transport the terrorists' weapons and ammunition.
- Maintaining control over the timing and logistics of the operation.
- Opting for the simplest method possible to minimize potential for miscalculations.
- Maximizing the chances of escape when the operation concludes.
- Minimizing the need to depend on good weather.

Step 3: Use this list to prioritize the ideas that were generated for each affinity group in the Structured Brainstorming session, placing the most likely choice for that group at the top of the list and the least likely at the bottom.

The students need to re-sort the lists they have generated. If the list is short, they can simply rearrange the ideas from most to least likely. If the list is long, then the students might first want to assign a rating to each idea, with 5 being the most likely and 1 being the least likely. If on further inspection some ideas should be dropped, they should receive a 0 and be deleted from the final list.

Another mechanism to prioritize the potential modes of transport is to have the students vote on which modes they believe are the most credible. A rule of thumb is to give each student one vote for every three possibilities. In this example, twenty modes of transport are listed, which means each student would have seven votes to distribute. It is recommended that the students be asked to write down their votes on 3 x 5 inch cards. The instructor then collects the cards, tallies the responses, and announces the results. If the students simply go to the whiteboard to mark their preferences, this could bias the results, as they might be inclined to vote for options that others have already selected.

Finally, they can use paired comparison, which is detailed in the section on Ranking, Scoring, Prioritizing in Heuer and Pherson (2015).[2]

Step 4: After prioritizing the ideas in each affinity group, generate a master list combining all of the lists. The most likely ideas overall should be at the top of the list and the least likely overall at the bottom.

Table 14.5 provides an example of how the final list could be rearranged. The most likely choices appear at the top with ratings of 5, 4, or 3. Credible but less likely ideas were given a score of 2 or 1. Those ideas receiving a 0, as

Table 14.5 ▶ Prioritized List of Ways to Enter Mumbai Example

Ways to Enter Mumbai	Rating
Take large boat to coast near Mumbai and transfer to small boats or Zodiacs.	5
Take large boat to coast near Mumbai and transfer to cars, truck, or taxis.	5
Conceal weapons in large commercial truck and accompany in personal cars.	4
Take large boat and transfer to submersible off coast of Mumbai.	4
Fly private aircraft to small airport near Mumbai and use a helicopter to enter city.	3
Hide in containers being transported by large cargo plane and sneak out.	3
Hide in large container ship and sneak out when arriving in harbor.	3
Drive personal vehicles to Mumbai.	2
Drive large commercial truck to Mumbai.	2
Take large boat from Pakistan directly to Port of Mumbai.	1
Rent large truck for land transport to Mumbai.	1
Take public ferry directly to Port of Mumbai.	1
Take private aircraft from India to Mumbai Airport.	0
Take bus to Mumbai.	0
Take train to Mumbai.	0
Hijack small aircraft to fly to Mumbai Airport.	0
Take private aircraft from Pakistan to Mumbai Airport.	0
Take commercial air from India to Mumbai Airport.	0
Take commercial air from Pakistan to Mumbai Airport.	0

not satisfying the criteria on further inspection, should be dropped from the final list.

Step 5: Once the group has articulated *how* it would have acted, ask it to explain *why* the group members think they would behave that way. Ask them to list what core values or core assumptions were motivating their behavior or actions. Again, this step establishes a baseline for assessing *why* the adversary is likely to react differently.

Step 6: Once the group can explain in a convincing way why it chose to act the way it did, ask the group members to put themselves in the shoes of the terrorists and simulate how they would respond, repeating Steps 2 to 4. Emphasize the need to avoid mirror imaging. The question now is not "What would you do if you were in their shoes?" but "How would the terrorists approach this problem, given their background, past experience, and the current situation?"

Step 7: At this point, after all the terrorists' ideas are gathered and prioritized, the group should ask, "Do the terrorists share our values or methods of operation?" If not, then how do those differences lead them to act in ways we might not have anticipated before engaging in this exercise?

Step 8: Present the results, describing the alternatives that were considered and the rationale for selecting the modes of transit the terrorists are most likely to choose. Consider less conventional means of presenting the results of the analysis, such as the following:

- Describing a hypothetical conversation in which the terrorists would discuss the issue in the first person.
- Drafting a document (set of instructions, military orders, or directives) that the leader of the terrorist group would likely generate.

Analytic Value Added: Was your list of criteria comprehensive? The list provided in Table 14.4 is fairly comprehensive, but challenging the students to come up with a few more ideas is always recommended. Terrorist groups can be very innovative, and surprise will work to their advantage.

Did some criteria deserve greater weight than others? Did you reflect this when you rated the various ideas? The process of rating each idea allows the students to reflect on the criteria they have developed. In this case, the concept of a staged transit appears to have the most utility. If traveling by sea, the assailants would need a larger ship that is ocean-worthy but then would have to transfer to some less visible mode of transit upon arriving in the vicinity of Mumbai.

Usually the students will propose to add criteria to the list. In this instance, one question would be whether the possibility of renting trucks (as has been done in the United States) or stealing them would be a viable option in India or Pakistan. Another issue that might arise is what strategy the terrorists have decided to adopt. If the intent is to launch a suicide bombing, then options using aircraft might be rated higher.

TECHNIQUE 3: CLASSIC QUADRANT CRUNCHING™

Classic Quadrant Crunching™ combines the methodology of a Key Assumptions Check[3] with Multiple Scenarios Generation[4] to generate an array of alternative scenarios or stories. This process is particularly helpful in the Mumbai case because little is known about the actual plans and intentions of the attackers. This technique helps the analyst identify and challenge key assumptions that may underpin the analysis while generating an array of credible alternative scenarios to help law enforcement focus on the most likely types of attacks to anticipate.

Task 3.

Use Classic Quadrant Crunching™ to brainstorm all the possible ways terrorists might launch an attack on Mumbai. List the scenarios from most to least likely.

Step 1: State your lead hypothesis.

This hypothesis should reflect either the consensus of the analytic unit regarding the most likely means of attack or the current conventional wisdom, which usually reflects how such attacks have been launched in the past. For illustrative purposes, we will use the hypothesis informed by the limited initial intelligence reporting received prior to the attack: Laškar-ĕ-Taiba (LeT) travels to Mumbai by (insert highest-ranked option listed in Task 2 or "by sea") and attacks the Taj Hotel with small arms and grenades, killing many people.

Step 2: Break the lead hypothesis down into its component parts based on the journalist's list of Who? What? How? When? Where? and Why?

Step 3: Identify which of these components are most critical to the analysis.

Step 4: For each of the critical components, identify two or four (an even number) contrary dimensions in a table, as shown in Table 14.6.

Six key components were identified in this exercise—one for each of the "five W's and H" questions. Three of the key components (not shaded in Table 10.7) deserve serious discussion and analysis because the contrary dimensions could pose significant new challenges for how best to defend the city.

Table 14.6 ▶ Defending Mumbai Classic Quadrant Crunching™: Contrary Dimensions Example

Key Components	Lead Hypothesis	Alternatives or Contrary Dimensions	
Who? (attacker)	Laškar-ĕ-Taiba (LeT)	Student Islamic Movement of India (SIMI)	Jaish-e-Mohammed (JEM)
What? (weapon)	Small arms and grenades	Small explosives	Large explosives
Where? (targets)	Taj Mahal Palace and other hotels	Transit locations (plane/train stations or airports) Western icons (businesses/restaurants)	Religious locations (temples, synagogues) Indian or Western government offices
How? (tactics)	A single event	Multiple simultaneous events	An extended event
Why? (motives)	To protest India as an enemy of Islam	To protest the West or the United States as an enemy of Islam	To protest Israel and Jews as enemies of Islam
When? (timing)	In the near future	On a significant date	A year from now

What? Historically, LeT has relied mostly on bombs, small arms, and grenades to generate large numbers of casualties. In several of its more spectacular actions, including its attacks on Indian forces in Kashmir, the strategy was to launch an assault deep into the target where the assailants then killed as many people as possible.[5] Since LeT has used a variety of weapons and tactics, a key question is this: What weapons would LeT employ in an attack on Mumbai? Would the use of small arms and grenades allow it to exact enough casualties? Would bombs generate more casualties? Would a large explosion (or several simultaneous explosions) attract more international attention?

Where? Would LeT consider attacking targets other than hotels? The initial intelligence mentions the Taj Mahal Palace Hotel as a primary target of the attack. It is a likely target but perhaps not the only one. Indian authorities in February 2008 had reported that a suspected terrorist, arrested in northern India, was found to possess drawings of various sites in Mumbai, some of which were targets in the November 2008 attack; these included the Taj Hotel and the Bombay Stock Exchange (which had also been a terrorist target in 1993). The Trident-Oberei Hotel was another prime candidate, as were other large public spaces such as railway stations and restaurants known to be frequented by foreigners. In the past, LeT has attacked Hindu temples. The organization's anti-Western and anti-Jewish rhetoric has also grown more intense in recent years. Indian and Western government offices and key infrastructure in Mumbai should not be ruled out as possible targets.

How? LeT has operated with different modi operandi over the years, opting for both simultaneous attacks and armed assaults against high-value targets. Historically, LeT has not conducted extended events or events including the taking of hostages, but this alternative is worth considering because an extended event, particularly if it involved a hostage taking, would advance several of the organization's key objectives—getting more international attention and deflecting criticism that it was engaging in indiscriminate violence.

The remaining questions are not good candidates for a Classic Quadrant Crunching™ exercise because either the alternatives to the lead hypotheses are not sufficiently likely to divert analytic resources or they would not have significant impact on how the analysis is conducted.

Who? A strong case can be made that LeT would be the prime candidate to launch the attack on Mumbai. A good analyst would challenge this assumption and consider other possible perpetrators. For example, another possibility could be Hindu radicals or a separatist group such as the Sikhs or the Tamils. For the purposes of illustrating this technique, however, we will assume that LeT is planning the attack. If a different group were to launch the attack, it probably would consider using the same range of weapons and tactics. The idea that the Pakistani government might be responsible for the attack or is providing support to the attackers is worth considering as a wildcard scenario. In this case, the key question is what support the attackers might receive from the Pakistanis that would significantly change the key attack scenarios.

When? This is important, but whether the attack is launched next week or next year would have little impact on how the analysis is conducted. The sense of urgency is already well established. The exercise raises a good question, however. Are there any particular dates that LeT would select that would further enhance its message?

Why? This question explores multiple motives for launching an attack. LeT sees India as part of the "Crusader-Zionist-Hindu" alliance and an enemy of Islam. Muslim-dominated Kashmir is ruled by the majority Hindu population of India, which provides LeT with a specific cause. LeT has increasingly portrayed its struggle in Kashmir as part of an international struggle. This justifies including foreigners (especially Britons and Americans) as targets as well as Jewish religious centers.

Step 5: Array combinations of these contrary assumptions in sets of 2 × 2 matrices.

For the purposes of this exercise, 2 × 2 matrices will be constructed based on the two What? (weapon) contrary dimensions, the two How? (tactics) contrary dimensions, and two of the four Where? (targets) contrary dimensions for a total of six contrary dimensions. These contrary dimensions then must be paired to create three different matrices with a total of twelve combinations. For ease of discussion, each quadrant has been given a number identifier. For example, in the first matrix, Quadrant 2 refers to an attack scenario involving large explosives and multiple events. The twelve possible combinations are shown in Table 14.7.

Step 6: Generate one or two credible scenarios for each quadrant.

For each cell in each matrix, generate one or two examples of how this scenario could play out. For example, in Quadrant 1, LeT attackers would orchestrate a series of small bombings. Some might be preplaced to go

Table 14.7 ▶ Mumbai Classic Quadrant Crunching™: 2 × 2 Matrices Examples

Weapon/Tactics			
1	Small explosives Multiple events	3	Small explosives Extended event
2	Large explosives Multiple events	4	Large explosives Extended event
Weapon/Locations			
5	Small explosives Transit locations	7	Small explosives Religious locations
6	Large explosives Transit locations	8	Large explosives Religious locations
Tactics/Locations			
9	Multiple events Transit locations	11	Extended event Transit locations
10	Multiple events Religious locations	12	Extended event Religious locations

off simultaneously in several hotels and the major train station, others would be thrown from motorcycles into large crowds, and even others would be set to kill police and other first responders who react to the initial set of bombings. In Quadrant 2, LeT would place large bombs or possibly suicide car or truck bombs at several iconic locations. Likely targets would include the Taj Hotel, Oberoi Hotel, train stations, and bus depots. In Quadrant 7, LeT assailants might place knapsacks filled with small explosives in a Jewish synagogue and time the detonation to go off during services. In Quadrant 10, they might launch multiple attacks at several key religious sites, including temples, synagogues, and Christian churches.

In some quadrants, the most likely scenario might be relatively easy to identify. In other quadrants, it could prove difficult to come up with a credible scenario. But several of the quadrants will usually stretch the analysts' thinking, forcing them to reframe the problem in a variety of ways. In so doing, they are almost certain to gain new insights and come up with a more creative set of potential attack scenarios.

Step 7: Array all the scenarios generated in a single list with the most credible scenario at the top of the list and the least credible at the bottom.

Review all the scenarios generated in Step 6 and select those most deserving of attention based on a preestablished set of criteria. In this example, possible criteria might include those scenarios that would create the most damage; generate the most publicity, especially on the world stage; or be the hardest to detect or prevent. This would include those scenarios most likely to capture the media's attention by attacking well-known icons or institutions, targeting foreigners, or extending the attack scenario over several days to give the media time to travel to Mumbai to cover the event.

Another way to narrow the list of scenarios is to remove those that make little or no sense. For example, a scenario involving large explosions as part of an extended event (Quadrant 4) may be beyond the capability of LeT. This scenario has been shaded in Table 14.7 to indicate it probably can be dropped.

Once the illogical scenarios are dropped, the next task is to prioritize the remaining scenarios. An illustrative list is provided in Table 14.8.

Analytic Value Added: **Which scenario is the most deserving of attention?** The scenario that received the highest score involved a series of simultaneous attacks replicating LeT's traditional reliance on an armed assault model.

Should attention focus on just one scenario, or could several scenarios play out simultaneously? Four of the attack scenarios received either a 4 or a 5 rating, suggesting that LeT might employ a variety of attack options or, at least, that Mumbai defenders should be prepared to defend against a broad array of attack options.

Are any key themes present when reviewing the most likely set of attention-deserving scenarios? Consideration of the contrary dimension of an extended event raises the possibility that the terrorists might take hostages as a means of gaining more publicity. Consideration of the large-explosion contrary dimension introduces the possibility of a large suicide car bomb or truck bomb. This option is less likely, however, given the logistical challenges of prepositioning such a bomb. The idea that insiders might be used to support either the planning of the attack or the actual attack scenario also emerges as a theme worth considering.

Does this technique help one determine where to devote the most attention in trying to deter the attack or mitigate the potential damage of the attack? The exercise suggests that more attention should be given to considering the hypotheses that several attack scenarios might be

Table 14.8 ▶ Mumbai Prioritized List of Alternative Scenarios Examples

Quadrant	Alternative Scenario	Rating
1	LeT launches simultaneous attacks using small arms and explosives targeting several hotels, the train station, and several restaurants.	5
3	LeT attacks the Taj Hotel with small arms and grenades and takes hostages; it also uses small explosives to set fire to the hotel.	4
10	LeT orchestrates a series of simultaneous attacks using small arms and grenades against Hindu temples and a Jewish synagogue, taking hostages at two of the locations.	4
5	LeT attacks the main train station, a bus depot, and people congregating at bus stops, throwing small explosives from motorcycles and setting small bombs in the train station.	4
9	LeT orchestrates a series of cascading attacks, beginning with small-arms fire and escalating to increasingly large bomb attacks targeting bus stops, bus depots, trains, and train stations.	3
11	LeT attacks the train station, takes hundreds of hostages, and sets up a defensive perimeter, leading to an extended siege.	3
2	LeT explodes several large suicide car bombs at hotels, the train station, and several restaurants.	2
7	LeT suicide bombers with vests attack several Hindu temples, a Jewish synagogue, and a Christian church.	2
12	LeT attacks a Jewish religious center or synagogue and takes hostages, leading to an extended siege.	2
6	Large bombs are detonated at a train station and the airport, causing major casualties.	1
8	LeT, with the support of insiders, explodes large preset bombs at various religious sites and then ambushes the first responders.	1

launched simultaneously instead of trying to predict exactly which scenario is most likely. Preparing for the possibility of several different attack scenarios also is a prudent approach when there is so much uncertainty.

TECHNIQUE 4: INDICATORS

Indicators are observable or deduced phenomena that can be periodically reviewed to track events, anticipate an adversary's plan of attack, spot emerging trends, distinguish among competing hypotheses, and warn of unanticipated change. An indicators list is a preestablished set of actions, conditions, facts, or events whose simultaneous occurrence would argue strongly that a phenomenon is present or about to be present or that a hypothesis is correct. The identification and monitoring of indicators are fundamental tasks of intelligence analysis, because they are the principal means of avoiding surprise. In the law enforcement community, indicators are used to assess whether a target's activities or behavior are consistent with an established pattern or lead hypothesis. These are often described as backward-looking or descriptive indicators. In intelligence analysis, indicators are often described as forward-looking or predictive indicators.

Preparation of a detailed indicator list by a group of knowledgeable analysts is usually a good learning experience for all participants. It can be a useful medium for an exchange of knowledge between analysts from different organizations or those with different types of expertise—for example, counterterrorism or counterdrug analysis, infrastructure protection, and country expertise. The indicator list can become the basis for conducting an investigation or directing collection efforts and routing relevant information to all interested parties. Identification and monitoring of indicators or signposts that a scenario is emerging can provide early warning of the direction in which the future is heading, but these early signs are not obvious. The human mind tends to see what it expects to see and to overlook the unexpected. Indicators take on meaning only in the context of a specific scenario with which they have been identified. The prior identification of a scenario and associated indicators can create an

awareness that prepares the mind to recognize and prevent a bad scenario from unfolding or help a good scenario to come about.

Task 4.

Create separate sets of indicators for the most attention-deserving scenarios, including those that were generated in Task 3, the Classic Quadrant Crunching™ exercise.

Step 1: Create a list of the most attention-deserving scenarios to track for this case.

Students should be encouraged to select the most attention-deserving scenarios, realizing that time is of the essence and the list should be kept short, preferably to no more than five scenarios. Usually that will require combining some scenarios that share similar characteristics. Table 14.9 provides an illustrative list of attention-deserving scenarios.

Table 14.9 ▶ Mumbai Most Attention-Deserving Scenarios Examples

Attention-Deserving Scenarios	Quadrants Represented
1. Simple armed assault. LeT conducts an armed assault with AK-47s and grenades launched from the sea against the Taj Hotel.	Lead Hypothesis
2. Simultaneous attacks. LeT launches simultaneous attacks from the sea using small arms and explosives targeting several hotels, a train station, religious sites, and restaurants.	1, 5, 9, 10
3. Suicide attacks. LeT orchestrates several simultaneous attacks launched from the sea using suicide bombers to target several public places, including hotels, a train station, and religious sites.	2, 7
4. Hostage taking. LeT attacks the Taj Hotel and possibly other sites from the sea, including those frequented by foreigners, with small arms and takes hostages.	3, 10, 11, 12

Step 2: Work alone, or preferably with a small group, to brainstorm a list of indicators for each scenario.

Step 3: Review and refine each set of indicators, as shown in Table 14.10, discarding any that are duplicative and combining those that are similar.

Step 4: Examine each indicator to determine if it meets the following five criteria. Discard those that are found wanting.

1. **Observable and collectible.** There must be some reasonable expectation that, if present, the indicator will be observed and reported by a reliable source. If an indicator is to monitor change over time, it must be collectible over time.
2. **Valid.** An indicator must be clearly relevant to the endstate the analyst is trying to predict or assess, and it must be inconsistent with all or at least some of the alternative explanations or outcomes. It must accurately measure the concept or phenomenon at issue.
3. **Reliable.** Data collection must be consistent when comparable methods are used. Those observing and collecting data must observe the same things. Reliability requires precise definition of the indicators.
4. **Stable.** An indicator must be useful over time to allow comparisons and to track events. Ideally, the indicator should be observable early in the evolution of a development so that analysts and decision makers have time to react accordingly.
5. **Unique.** An indicator should measure only one thing and, in combination with other indicators, should point only to the phenomenon being studied. Valuable indicators are those that not only are consistent with a specified scenario or hypothesis but also are inconsistent with all other alternative scenarios.

Several indicators relating to tracking the purchase of guns, grenades, and ammunition would be very hard to observe (1-f, 2-d, 3-f, and 4-d). LeT probably has its own well-established supply links, and its purchases would not stand out from the ubiquitous trafficking of arms in Pakistan.

Analytic Value Added: Are the indicators mutually exclusive and comprehensive? The indicators focus primarily on preparations for launching an attack and what locations might be targeted. Other indicators with merit include those indicating how the attackers plan to transport themselves to Mumbai and those that might prove unique to a specific target location.

Table 14.10 ▶ Mumbai Indicators for Most Attention-Deserving Scenarios Examples

Number	Attention-Deserving Scenario
Scenario 1, Simple Armed Assault: LeT conducts an armed assault with AK-47s and grenades launched from the sea against the Taj Hotel.	
1-a	Sources report LeT is providing small arms/grenades training in Pakistan.
1-b	Suspicious people are only observed surveilling the Taj Mahal Palace.
1-c	People renting rooms at the Taj Mahal Palace for several weeks appear suspicious.
1-d	Sources report that Taj Mahal Palace is a primary target.
1-e	LeT posts anti-Indian rhetoric on its website.
1-f	Reports tell of LeT purchases of assault rifles, grenades, and ammunition in Pakistan.
1-g	Sources report that the attack team is small (five or fewer people).
1-h	Small-arms caches are discovered in or around Mumbai.
1-i	Documents captured in LeT possession show sketches of only the Taj Hotel.
Scenario 2, Simultaneous Attacks: LeT launches simultaneous attacks from the sea using small arms and explosives targeting several hotels, a train station, religious sites, and restaurants.	
2-a	Sources report LeT is providing training in small arms, portable bombs, preset bombs, and grenades at camps in Pakistan.
2-b	Suspicious people are observed surveilling a large number of prominent public sites in Mumbai.
2-c	LeT posts anti-Indian rhetoric on its website.
2-d	Reports tell of LeT purchases or acquisition of assault rifles, grenades, and ammunition.
2-e	Reports tell of LeT purchases or acquisition of RDX and other bomb materials.
2-f	Sources report the attackers are formed into several teams and number more than five.
2-g	Possible trial runs are observed in the streets of Mumbai.
2-h	Target organizations or facilities report receiving threats of imminent attack.
2-i	Documents captured in LeT possession suggest several possible targets.
Scenario 3, Suicide Attacks: LeT orchestrates several simultaneous attacks launched from the sea using suicide bombers to target several public places, including hotels, the train station, and religious sites.	
3-a	Sources report LeT is recruiting suicide bombers.
3-b	Sources report LeT is providing training in the use of suicide vests or it is practicing deploying suicide car or truck bombs.
3-c	Sources report LeT supporters are conducting practice suicide bombings.
3-d	Suspicious people are observed surveilling a large number of prominent public sites in Mumbai.
3-e	LeT posts virulent anti-Indian rhetoric on its website justifying the use of suicide bombers.
3-f	Reports tell of LeT purchases or acquisition of materials used by suicide bombers.
3-g	Sources report the attack team is comprised of only a handful of people.
3-h	Sources report little emphasis on small-arms training in LeT camps.
3-i	LeT releases martyrdom videos.
Scenario 4, Hostage Taking: LeT attacks the Taj Hotel and possibly other sites from the sea, including those frequented by foreigners, with small arms and takes hostages.	
4-a	Sources report LeT is providing small-arms training in Pakistan.
4-b	Suspicious people are observed surveilling sites often frequented by foreigners.
4-c	LeT websites emphasize the international aspects of the organization's struggle.

(Continued)

Table 14.10 ▶ Mumbai Indicators for Most Attention-Deserving Scenarios Examples *(Continued)*

Number	Attention-Deserving Scenario
4-d	Reports tell of LeT purchases or acquisition of large amounts of ammunition.
4-e	Sources report the attackers are formed into several teams.
4-f	Suspicious people are observed surveilling Western businesses, synagogues, churches.
4-g	Intelligence reports suggest an operation lasting several days.
4-h	Sources report that LeT operatives will carry handcuffs, tape, phones in their packs.
4-i	Sources report that LeT is scouting for locations that can be easily defended.
4-j	Sources report that LeT camps are providing training in defending fixed positions.

Have a sufficient number of high-quality indicators been generated for each scenario to enable an effective analysis? At least nine indicators were developed for each scenario. Most brainstorming sessions usually generate a higher number because of the different perspectives being brought to the table. However, as the quantity of indicators goes up, their quality often decreases.

Can the indicators be used to help detect a planned attack or deter a possible hostile course of action? Several of the indicators suggest potentially productive avenues for Mumbai police investigators. For example, countersurveillance teams could be dispatched to high-value targets such as the Taj Hotel, the train station, and other hotels and restaurants often frequented by foreigners.

TECHNIQUE 5: INDICATORS VALIDATOR™

The Indicators Validator™ is a simple tool for assessing the diagnostic power of indicators. Once an analyst has developed a set of attention-deserving alternative scenarios or competing hypotheses, the next step is to generate indicators for each scenario or hypothesis that would appear if that particular scenario were beginning to emerge or that particular hypothesis were true. A critical question that is not often asked is whether a given indicator would appear only for the scenario or hypothesis to which it is assigned or also in one or more alternative scenarios or hypotheses. Indicators that could appear under several scenarios or hypotheses are not considered diagnostic; that is, they are not particularly useful in determining whether a specific scenario is beginning to emerge or a particular hypothesis is true. The ideal indicator is highly likely for the scenario to which it is assigned and highly unlikely for all others.

Task 5.

Use the Indicators Validator™ to assess the diagnosticity of your indicators.

Step 1: Create a matrix similar to that used for Analysis of Competing Hypotheses.[6] This can be done manually or by using the Indicators Validator™ software. Contact Globalytica, LLC at THINKSuite@globalytica.com or go to http://www.globalytica.com to obtain access to the Indicators Validator™ software if it is not available on your system. List the alternative scenarios along the top of the matrix and the indicators that have been generated for each of the scenarios down the left side of the matrix.

Step 2: Moving across the indicator rows, assess whether the indicator for each scenario

- Is highly likely to appear
- Is likely to appear
- Could appear
- Is unlikely to appear
- Is highly unlikely to appear

Indicators developed for their particular scenario, the home scenario, should be either highly likely or likely.

If the software is unavailable, you can do your own scoring. If the indicator is *highly likely* in the home scenario, then in the other scenarios,

- Highly likely is 0 points.
- Likely is 1 point.

- Could is 2 points.
- Unlikely is 4 points.
- Highly unlikely is 6 points.

If the indicator is *likely* in the home scenario, then in the other scenarios,

- Highly likely is 0 points.
- Likely is 0 points.
- Could is 1 point.
- Unlikely is 3 points.
- Highly unlikely is 5 points.

Step 3: Tally up the scores across each row and then rank order all the indicators.

Table 14.11 shows how each indicator was rated for each scenario. The number beside the rating is the score. It is important to remind the students that the scoring for "home scenario" indicators rated likely is different from the scoring for "home scenario" indicators rated highly likely. The total score for each indicator is shown in the column on the far right.

Step 4: Re-sort the indicators, putting those with the highest total score at the top of the matrix and those with the lowest score at the bottom. The most discriminating indicator is highly likely to emerge under the home scenario and highly unlikely to emerge under all other scenarios. The least discriminating indicator is highly likely to appear in all scenarios. Most indicators will fall somewhere in between.

Step 5: The indicators with the most highly unlikely and unlikely ratings are the most discriminating and should be retained.

Step 6: Indicators with no highly unlikely or unlikely ratings should be discarded.

Step 7: Use your judgment as to whether you should retain or discard indicators that score fewer points. Generally, you should discard all indicators that have no highly unlikely or

Table 14.11 ▶ Mumbai Indicators Validator™ Scoring Examples

Number	Indicator	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Score
Scenario 1, Simple Armed Assault: LeT conducts an armed assault with AK-47s and grenades launched from the sea against the Taj Hotel.						
1-a	Sources report LeT is providing small arms/grenades training in Pakistan.	HL	HL (0)	L (1)	HL (0)	1
1-b	Suspicious people are only observed surveilling the Taj Mahal Palace.	HL	HL (0)	HL (0)	HL (0)	0
1-c	People renting rooms at the Taj Mahal Palace for several weeks appear suspicious.	HL	L (1)	L (1)	HL (0)	2
1-d	Sources report that Taj Mahal Palace is a primary target.	HL	HL (0)	HL (0)	HL (0)	0
1-e	LeT posts anti-Indian rhetoric on its website.	L	L (0)	L (0)	L (0)	0
1-h	Small-arms caches are discovered in or around Mumbai.	L	L (0)	C (1)	L (0)	1
1-i	Documents captured in LeT possession show sketches of only the Taj Hotel.	HL	U (4)	U (4)	C (2)	10
Scenario 2, Simultaneous Attacks: LeT launches simultaneous attacks from the sea using small arms and explosives targeting several hotels, a train station, religious sites, and restaurants.						
2-a	Sources report LeT is providing training in small arms, portable bombs, preset bombs, and grenades at camps in Pakistan.	C (2)	HL	U (4)	HL (0)	6
2-b	Suspicious people are observed surveilling a large number of prominent public sites in Mumbai.	U (3)	L	L (0)	L (0)	3
2-c	LeT posts anti-Indian rhetoric on its website.	L (0)	L	L (0)	L (0)	0

(Continued)

Table 14.11 ▶ Mumbai Indicators Validator™ Scoring Examples *(Continued)*

Number	Indicator	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Score
2-e	Reports tell of LeT purchases or acquisition of RDX and other bomb materials.	HU (6)	HL	L (1)	L (1)	8
2-f	Sources report the attackers are formed into several teams and number more than five.	U (4)	HL	C (2)	C (2)	8
2-h	Target organizations or facilities report receiving threats of imminent attack.	U (3)	L	C (1)	C (1)	5
2-i	Documents captured in LeT possession suggest several possible targets.	U (3)	HL	C (2)	C (2)	7
	Scenario 3, Suicide Attacks: LeT orchestrates several simultaneous attacks launched from the sea using suicide bombers to target several public places, including hotels, the train station, and religious sites.					
3-a	Sources report LeT is recruiting suicide bombers.	U (4)	U (4)	HL	HU (6)	14
3-b	Sources report LeT is providing training in the use of suicide vests or it is practicing deploying suicide car or truck bombs.	HU (6)	HU (6)	HL	HU (6)	18
3-c	Sources report LeT supporters are conducting practice suicide bombings.	HU (6)	HU (6)	HL	HU (6)	18
3-d	Suspicious people are observed surveilling a large number of prominent public sites in Mumbai.	U (3)	HL (0)	L	HL (0)	3
3-e	LeT posts virulent anti-Indian rhetoric on its website justifying the use of suicide bombers.	U (4)	L (1)	HL	C (2)	7
3-h	Sources report little emphasis on small-arms training in LeT camps.	HU (5)	HU (5)	L	HU (5)	15
3-i	LeT releases martyrdom videos.	U (3)	U (4)	L	U (4)	11
	Scenario 4, Hostage Taking: LeT attacks the Taj Hotel and possibly other sites from the sea, including those frequented by foreigners, with small arms and takes hostages.					
4-a	Sources report LeT is providing small-arms training in Pakistan.	HL (0)	HL (0)	L (1)	HL	1
4-b	Suspicious people are observed surveilling sites often frequented by foreigners.	L (0)	HL (0)	L (0)	L	0
4-c	LeT websites emphasize the international aspects of the organization's struggle.	HL (0)	HL (0)	L (1)	HL	1
4-e	Sources report the attackers are formed into several teams.	U (2)	HL (0)	C (1)	L	3
4-f	Suspicious people are observed surveilling Western businesses, synagogues, churches.	U (4)	HL (0)	HL (0)	HL	4
4-g	Intelligence reports suggest an operation lasting several days.	U (4)	C (2)	HL (0)	HL	6
4-h	Sources report that LeT operatives will carry handcuffs, tape, phones in their packs.	U (2)	U (2)	U (2)	L	6
4-i	Sources report that LeT is scouting for locations that can be easily defended.	U (2)	C (1)	U (2)	L	5
4-j	Sources report that LeT camps are providing training in defending fixed positions.	U (2)	U (2)	U (2)	L	6

Note: HL = highly likely to appear; L = likely to appear; C = could appear; U = unlikely to appear; HU = highly unlikely to appear.

unlikely ratings. In some cases, an indicator may be worth keeping if it is useful when viewed in combination with several other indicators.

As shown in Table 14.12, the following indicators should be discarded because of their low point score and lack of any unlikely or highly unlikely ratings: 1-c (2 points); 1-a, 1-h, 4-a, and 4-c (1 point); and 1-b, 1-d, 1-e, 2-c, and 4-b (0 points). Several indicators have scores of 3 (2-b, 3-d, and 4-e) but were retained because the indicator was rated as unlikely for at least one scenario.

Table 14.12 ▶ Mumbai Ordering Indicators by Diagnosticity Example

Number	Indicator	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Score
3-b	Sources report LeT is providing training in the use of suicide vests or it is practicing deploying suicide car or truck bombs.	HU (6)	HU (6)	HL	HU (6)	18
3-c	Sources report LeT supporters are conducting practice suicide bombings.	HU (6)	HU (6)	HL	HU (6)	18
3-h	Sources report little emphasis on small-arms training in LeT camps.	HU (5)	HU (5)	L	HU (5)	15
3-a	Sources report LeT is recruiting suicide bombers.	U (4)	U (4)	HL	HU (6)	14
3-i	LeT releases martyrdom videos.	U (3)	U (4)	L	U (4)	11
1-i	Documents captured in LeT possession show sketches of only the Taj Hotel.	HL	U (4)	U (4)	C (2)	10
2-e	Reports tell of LeT purchases or acquisition of RDX and other bomb materials.	HU (6)	HL	L (1)	L (1)	8
2-f	Sources report the attackers are formed into several teams and number more than five.	U (4)	HL	C (2)	C (2)	8
2-i	Documents captured in LeT possession suggest several possible targets.	U (3)	HL	C (2)	C (2)	7
3-e	LeT posts virulent anti-Indian rhetoric on its website justifying the use of suicide bombers.	U (4)	L (1)	HL	C (2)	7
2-a	Sources report LeT is providing training in small arms, portable bombs, preset bombs, and grenades at camps in Pakistan.	C (2)	HL	U (4)	HL (0)	6
4-g	Intelligence reports suggest an operation lasting several days.	U (4)	C (2)	HL (0)	HL	6
4-h	Sources report that LeT operatives will carry handcuffs, tape, phones in their packs.	U (2)	U (2)	U (2)	L	6
4-j	Sources report that LeT camps are providing training in defending fixed positions.	U (2)	U (2)	U (2)	L	6
2-h	Target organizations or facilities report receiving threats of imminent attack.	U (3)	L	C (1)	C (1)	5
4-i	Sources report that LeT is scouting for locations that can be easily defended.	U (2)	C (1)	U (2)	L	5
4-f	Suspicious people are observed surveilling Western businesses, synagogues, churches.	U (4)	HL (0)	HL (0)	HL	4
2-b	Suspicious people are observed surveilling a large number of prominent public sites in Mumbai.	U (3)	L	L (0)	L (0)	3

(Continued)

Table 14.12 ▶ Mumbai Ordering Indicators by Diagnosticity Example *(Continued)*

Number	Indicator	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Score
3-d	Suspicious people are observed surveilling a large number of prominent public sites in Mumbai.	U (3)	HL (0)	L	HL (0)	3
4-e	Sources report the attackers are formed into several teams.	U (2)	HL (0)	C (1)	L	3
1-c	People renting rooms at the Taj Mahal Palace for several weeks appear suspicious.	HL	L (1)	L (1)	HL (0)	2
1-a	Sources report LeT is providing small-arms/grenades training in Pakistan.	HL	HL (0)	L (1)	HL (0)	1
1-h	Small-arms caches are discovered in or around Mumbai.	L	L (0)	C (1)	L (0)	1
4-a	Sources report LeT is providing small-arms training in Pakistan.	HL (0)	HL (0)	L (1)	HL	1
4-c	LeT websites emphasize the international aspects of the organization's struggle.	HL (0)	HL (0)	L (1)	HL	1
1-b	Suspicious people are only observed surveilling the Taj Mahal Palace.	HL	HL (0)	HL (0)	HL (0)	0
1-d	Sources report that Taj Mahal Palace is a primary target.	HL	HL (0)	HL (0)	HL (0)	0
1-e	LeT posts anti-Indian rhetoric on its website.	L	L (0)	L (0)	L (0)	0
2-c	LeT posts anti-Indian rhetoric on its website.	L (0)	L	L (0)	L (0)	0
4-b	Suspicious people are observed surveilling sites often frequented by foreigners.	L (0)	HL (0)	L (0)	L	0

Note: HL = highly likely to appear; L = likely to appear; C = could appear; U = unlikely to appear; HU = highly unlikely to appear.

Step 8: Once nondiscriminating indicators have been eliminated, regroup the indicators under their home scenarios.

Overall, twenty indicators were deemed diagnostic, and ten were discarded as not sufficiently diagnostic to be useful in the analysis. When these twenty indicators are re-sorted by scenario, as shown in Table 14.13, it is immediately apparent that there is an insufficient number of diagnostic indicators for Scenario 1, Simple Armed Assault.

Step 9: If a large number of indicators for a particular scenario have been eliminated, develop additional—and more diagnostic—indicators for that scenario.

Step 10: Recheck the diagnostic value of any new indicators by applying the Indicators Validator™ to them as well.

In this case, students should generate a new set of diagnostic indicators for Scenario 1. The problem confronted when trying to come up with Scenario 1 indicators is that the scenario is a fairly basic scenario and most of its elements would be incorporated into the attack plans in the other scenarios. The indicators that were listed would help an analyst confirm that, at a minimum, planning was underway for an attack on the Taj Hotel by sea or that LeT was developing a capability to launch such an attack. Intelligence sources, however, have already indicated that such an attack is being contemplated. Given that circumstance, the indicators would confirm what has already been reported but would not distinguish the type of attack being contemplated. Any new indicators for Scenario 1 should probably focus on activities or statements indicating that more sophisticated attacks have been ruled out, such as the following:

- LeT communications indicate that efforts to recruit suicide bombers have failed.
- LeT communications underscore the need to keep the operation as simple as possible to ensure its success.

Table 14.13 ▶ Mumbai Diagnostic Indicators by Scenario Example

Number	Indicator	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Score
Scenario 1, Simple Armed Assault: LeT conducts an armed assault with AK-47s and grenades launched from the sea against the Taj Hotel.						
1-i	Documents captured in LeT possession show sketches of only the Taj Hotel.	HL	U (4)	U (4)	C (2)	10
Scenario 2, Simultaneous Attacks: LeT launches simultaneous attacks from the sea using small arms and explosives targeting several hotels, a train station, religious sites, and restaurants.						
2-e	Reports tell of LeT purchases or acquisition of RDX and other bomb materials.	HU (6)	HL	L (1)	L (1)	8
2-f	Sources report the attackers are formed into several teams and number more than five.	U (4)	HL	C (2)	C (2)	8
2-i	Documents captured in LeT possession suggest several possible targets.	U (3)	HL	C (2)	C (2)	7
2-a	Sources report LeT is providing training in small arms, portable bombs, preset bombs, and grenades at camps in Pakistan.	C (2)	HL	U (4)	HL (0)	6
2-h	Target organizations or facilities report receiving threats of imminent attack.	U (3)	L	C (1)	C (1)	5
2-b	Suspicious people are observed surveilling a large number of prominent public sites in Mumbai.	U (3)	L	L (0)	L (0)	3
Scenario 3, Suicide Attacks: LeT orchestrates several simultaneous attacks launched from the sea using suicide bombers to target several public places, including hotels, a train station, and religious sites.						
3-b	Sources report LeT is providing training in the use of suicide vests or it is practicing deploying suicide car or truck bombs.	HU (6)	HU (6)	HL	HU (6)	18
3-c	Sources report LeT supporters are conducting practice suicide bombings.	HU (6)	HU (6)	HL	HU (6)	18
3-h	Sources report little emphasis on small arms training in LeT camps.	HU (5)	HU (5)	L	HU (5)	15
3-a	Sources report LeT is recruiting suicide bombers.	U (4)	U (4)	HL	HU (6)	14
3-i	LeT releases martyrdom videos.	U (3)	U (4)	L	U (4)	11
3-e	LeT posts virulent anti-Indian rhetoric on its website justifying the use of suicide bombers.	U (4)	L (1)	HL	C (2)	7
3-d	Suspicious people are observed surveilling a large number of prominent public sites in Mumbai.	U (3)	HL (0)	L	HL (0)	3
Scenario 4, Hostage Taking: LeT attacks the Taj Hotel and possibly other sites from the sea, including those frequented by foreigners, with small arms and takes hostages.						
4-g	Intelligence reports suggest an operation lasting several days.	U (4)	C (2)	HL (0)	HL	6
4-h	Sources report that LeT operatives will carry handcuffs, tape, phones in their packs.	U (2)	U (2)	U (2)	L	6
4-j	Sources report that LeT camps are providing training in defending fixed positions.	U (2)	U (2)	U (2)	L	6
4-i	Sources report that LeT is scouting for locations that can be easily defended.	U (2)	C (1)	U (2)	L	5
4-f	Suspicious people are observed surveilling Western businesses, synagogues, churches.	U (4)	HL (0)	HL (0)	HL	4
4-e	Sources report the attackers are formed into several teams.	U (2)	HL (0)	C (1)	L	3

Note: HL = highly likely to appear; L = likely to appear; C = could appear; U = unlikely to appear; HU = highly unlikely to appear.

- Sources report that only small numbers of weapons and small amounts of ammunition will be used in the operation.

Analytic Value Added: Does each scenario have a robust set of highly diagnostic indicators? A good start has been made at developing a set of diagnostic indicators, but additional brainstorming should generate a more robust set. This would suggest that other experts be brought in to help brainstorm, especially those familiar with LeT or these types of terrorist operations.

Do these indicator lists provide useful leads for alerting local officials and businesspeople, such as hotel and restaurant owners, of plausible attack scenarios? Are the indicators focused enough to generate specific collection requirements or follow-on tasking by giving local officials and businesspeople a more concrete idea of what to look for? The indicators provide many useful leads for law enforcement analysts as well as a good set of questions analysts can share with the management and chiefs of security at likely target locations, including the Taj Hotel, train stations, various high-visibility Western establishments, and public places often frequented by foreigners.

CONCLUSION

A group of Laškar-ě-Taiba (LeT) operatives ultimately launched a coordinated attack on multiple targets across Mumbai on 26 November 2008 (see Map 14.2). The assailants quietly entered the country by sea and used small arms and explosive devices to attack transportation infrastructure, hotels, other businesses, and a religious site. Sources differ as to how many casualties occurred during the attacks, but a survey of several estimates makes it clear that more than 160 people died and over 300 suffered wounds over the course of the 60-hour rampage.[7] Twenty-six of the dead were foreigners, including six Americans.[8]

Additional Intelligence Reporting

During the month between the initial threat report from the United States and the day of the attack, the Indian government—aided by the United States—diligently tracked down additional information about the plot. In early November, the Indian Intelligence Bureau intercepted communications from a leader of LeT in Pakistan that referred to an attack against hotels in Mumbai.[9] US intelligence provided additional information about LeT's plans to attack the Taj Hotel and other sites frequented by foreigners and Americans.[10] On 19 November, the Indian intelligence service uncovered information that a suspicious ship might be en route to Mumbai and that an attack on the city was imminent.[11, 12]

The Journey to Mumbai

A group of ten men belonging to LeT boarded a ship in Karachi at 0800 on 22 November 2008 and headed out to

Map 14.2 ▶ Targets of Mumbai Terrorist Attack, 26 November 2008

sea to rendezvous with the *Al-Husseini*, a vessel owned by Zaki-ur-Rehman, a LeT commander.[13, 14] The following day, the *Al-Husseini* encountered a 45-foot fishing trawler named the *Kuber*.[15] It is unclear whether the meeting between the two ships on the Arabian Sea was prearranged or happened by chance. The *Kuber* was boarded by LeT militants and captured. Four of the *Kuber*'s crewmembers were transferred to the *Al-Husseini* and killed.[16] Only Amar Singh Solanki, the *Kuber*'s captain, was left aboard the hijacked ship. Indian officials believe that Solanki helped pilot the trawler to Mumbai, which lay some 550 nautical miles from the point where the two ships met.[17]

It is unknown exactly how many LeT operatives traveled aboard the *Kuber* to Mumbai, but Indian investigators collected enough personal articles for at least fifteen people.[18] A satellite phone recovered from the ship revealed that the group aboard the fishing vessel kept in close contact with Rehman and other senior LeT officials during the voyage to India. While on board the trawler, each of the ten men who met the *Al-Husseini* off Karachi were given individual bags containing a Kalashnikov, a 9 mm pistol, ammunition, grenades, and an improvised explosive device (IED) made with a military-grade explosive known as RDX.[19] On 26 November, the *Kuber* reached the coast of Mumbai, reduced its speed, and idled until darkness fell. In one of the final telephone calls before the attack began, an unknown LeT official in Pakistan instructed the men to kill the ship's captain. After the call ended, the militants followed their orders and beheaded Solanki.[20]

The Assault

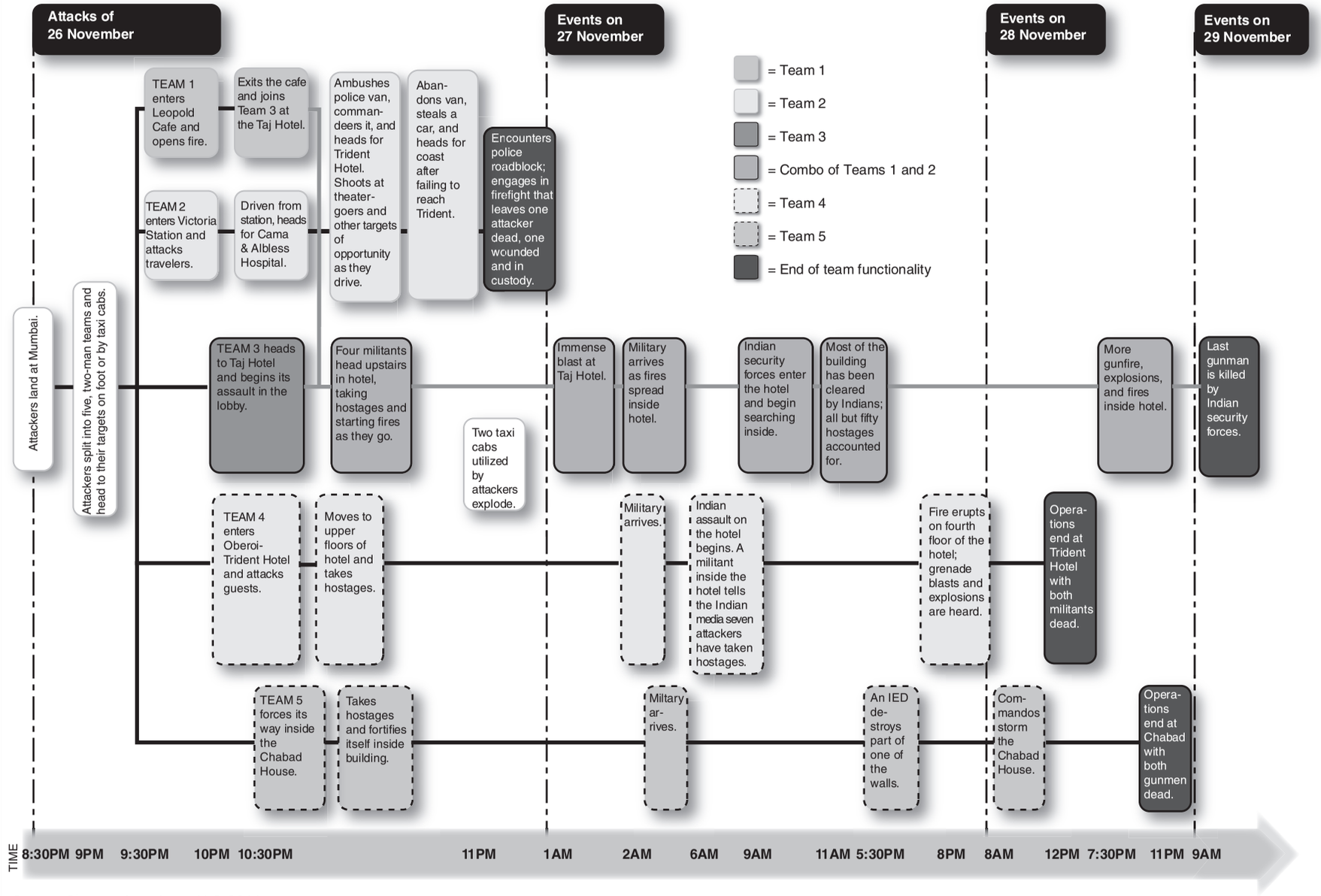
Indian officials believe the LeT men came ashore on the night of 26 November in an inflatable boat that landed near Badhwar Park in South Mumbai.[21] Other sources contend the attackers used two inflatable boats and arrived separately at Badhwar Park and the Apollo Bunder Fishing Docks.[22] Upon arrival, the militants divided themselves into five teams of two gunmen and then proceeded toward their targets, all of which appear to have been selected in advance.[23] An interrogation of one of the terrorists conducted after the attacks revealed that extensive surveillance of the targets had been conducted in the months leading up to the assault. In some cases, LeT operatives had even rented rooms in the hotels the group was interested in targeting to gather details about each building's layout.[24] In at least two cases, attackers utilized public taxis to approach their target.[25] Bombs were left in both taxis by the terrorists, and both later exploded, killing the two drivers and at least one bystander.[26]

The ten militants were briefed in Pakistan using digital photos and maps obtained from the Internet to familiarize them with the city's layout and the locations of their targets. Meanwhile, LeT had set up a remote command post in a safe house or hotel that Indian officials believed was in Lahore or Karachi, Pakistan. The safe house was filled with computers, televisions, voice-over-Internet phones (VOIP), and satellite phones manned by six LeT terrorists who maintained contact with the terrorist teams as they moved through the city.[27]

There is no definitive account of which attack occurred first, but one of the earliest reports of violence came from the Leopold Café, a historic restaurant and watering hole popular with foreigners and locals.[28] Shortly after 2100, Hafiz Ashad and Naser entered the Leopold and began spraying the patrons inside with machine-gun fire.[29] One of the two men also lobbed a grenade into the tightly packed café. According to one eyewitness account, the assault began with what sounded like a light bulb shattering, and then "screams erupted as the crowded restaurant was raked with gunfire."[30] Photos from the attack show bullet holes in the café window and the walls and other damage from the explosion.[31] Indian investigators say the terrorists remained inside the Leopold for about five minutes, during which time they killed ten people—among them two Americans—prior to heading toward the Taj Mahal Palace Hotel.[32]

At about the same time diners were under attack at the Leopold, Abu Ismail Khan and Mohammad Ajmal Kasab entered the crowded Chhatrapati Shivaji Terminus—or Victoria Station—and began firing indiscriminately at people on the platforms.[33] "I was firing and Abu was hurling hand grenades," Kasab later recalled in court.[34] "I was in front of Abu who had taken such a position that no one could see him. I fired at a policeman after which there was no firing from the police's side." A total of 58 people died and 104 were injured before a small band of police drove the attackers from the station's terminal.[35] Outside, the two militants fled across a pedestrian bridge and headed toward the Cama & Albless Hospital. Together, the pair ambushed a van carrying police officers and counterterrorism officials, killing six out of the seven law enforcement officials riding inside. Wrongly believing all of the vehicle's occupants were dead, the militants dumped several of the bodies on the road and then commandeered the van for themselves. Constable Arun

Figure 14.1 ▶ Timeline of Mumbai Attacks and Aftermath, 26–29 November 2008



Source: Pherson Associates, LLC, 2011.

Jadhav, the only officer who survived the attack, switched on his radio and transmitted live audio from the back of the vehicle as the militants careened through the streets, shooting at targets of opportunity.[36] Jadhav said the two men in the van also fired at police officers as they drove: "One of them laughed and said, 'Look, they're wearing [bulletproof] jackets,'" after killing one such officer.[37]

When the van approached the Metrobig Cinemas, the gunmen slowed the vehicle's speed and opened fire on the large crowd gathered on the sidewalk, killing ten people.[38] The duo then attempted to reach the Oberoi-Trident Hotel but was turned back by police barricades.[39] When the van developed a flat tire, they abandoned it and stole a Skoda automobile.[40] The pair headed toward the sea with unknown intent. Their journey was halted when they encountered a roadblock at Girgaum Chowpatti and became involved in a firefight with police that left Khan dead and Kasad—the attack's only survivor—wounded and in police custody.

The third LeT team—Shoaib and Javad—sprinted into the lobby of the Taj Mahal Palace Hotel, an iconic building located near the city's waterfront that attracts an elite clientele of businesspeople and holiday travelers, and began firing into the crowded room.[41] "A gunman just stood there spraying bullets around, right next to me," said Sajjad Karim, a British diplomat who was inside the hotel during the attack.[42] "I managed to turn away and I ran into the hotel kitchen. . . . All of a sudden another gunman appeared in front of us, carrying machine gun-type weapons. And he just started firing at us. . . . I just turned and ran in the opposite direction." Firing wildly and tossing grenades, the gunmen managed to kill about twenty people in the first few minutes of their assault.[43] Shortly after the attack began, the LeT team that attacked the Leopold Café—Ashad and Naser—arrived in the lobby of the Taj Hotel and added their firepower to the carnage already unfolding. Together, the four militants ascended to the upper floors of the hotel to round up hostages and fortify their position.

The fourth LeT team—Abdul Rehman Chotta and Fahadullah—entered the Oberoi-Trident Hotel through the main doors about fifteen minutes after the attack began at the Taj Hotel.[44] After the militants peppered the hotel's restaurant with machine-gun fire, they ignited their IEDs and shot at whoever had not escaped from the lobby. "We took the lift to the lobby and heard bangs as the door opened," a British business traveler remembered.[45] "A Japanese man, one of four men in the lift, was shot and wounded. I frantically pressed the 'close door' button but had to move the shot man's foot for the doors to close." As was the case at the Taj Hotel, after the initial burst of violence and killing, the attackers headed for the hotel's upper floors, collected hostages, and prepared themselves for a response from the Indian security forces gathering outside.

The fifth and final LeT attack team—Babar Imran and Nazir—assaulted a community center owned and operated by Chabad Lubavich, a Hasidic outreach movement.[46] The five-story building housed a rabbi and catered almost exclusively to Jews visiting India. Unlike the other targets, the Chabad House was not a well-known landmark and was frequented neither by businesspeople nor Westerners.[47] The attackers targeted the building because they were "told by their handlers in Pakistan that the lives of Jews were worth 50 times those of non-Jews." A spokesperson for the Chabad group said Rabbi Gavriel Noach Holtzberg, age twenty-nine, telephoned the Israeli consulate to report gunmen had entered the facility.[48] "In the middle of the conversation, the line went dead," the spokesperson said. Both Holtzberg and his wife were killed sometime during the attack. According to an account from an unidentified medic who entered the center shortly after the Indian government killed the attackers, many of the Jews in the house survived Imran and Nazir's initial raid and subsequently "were tortured very badly."[49]

At the end of the initial assaults on 26 November, four of the five LeT attack teams were still operational. One terrorist was dead and another had been captured, but the remaining eight militants had all taken hostages and strengthened their positions inside the Chabad House and the Taj and Oberoi Hotels. Sporadic gunfire between the growing number of Indian security forces gathering outside and the terrorists occurred throughout the night and into the early morning of 27 November. During this same period, Mumbai's first responders, a mixture of police officers and local counterterrorism officials, were seconded—or replaced entirely—by military forces.[50] The National Security Guards (NSG), India's elite commando force, also arrived from New Delhi.

Throughout the standoff at the Taj Hotel and the other two locations, the militants used cellular phones to keep in contact with LeT commanders in Pakistan, who were monitoring events in Mumbai by watching Indian television coverage.[51] The LeT commanders told the terrorists occupying the Taj Hotel to set fires so that people could see the hotel burn on television, suggesting that the attack was choreographed with media coverage in mind.[52]

Box 14.3 THE MUMBAI ASSAILANTS

Team 1: Hafiz Ashad and Naser attack the Leopold Café near the Taj Mahal Palace Hotel. They spend five to ten minutes in café, toss a grenade into the crowd of diners, then head for the Taj to join up with their comrades. At the Taj Hotel, they head to the upper floors with members of Team 3 and help take hostages. Both die when Indian security forces assault the Taj Hotel.

Team 2: Mohammad Ajmal Kasab and Abu Ismail Khan assault the Chhatrapati Shivaji Terminus and are forced to flee outside after they encounter the police. They move to the Cama and Albless Hospital where they ambush a police van, steal it, and attempt to drive to the Oberoi-Trident Hotel. The team is prevented from reaching the hotel by a police roadblock. The pair abandon the police van and then steal another car. At Girgaum Chowpatti, a shootout ensues with police that ends with Khan dead and Kasab in police custody.

Team 3: Shoaib and Javad head directly to the Taj Hotel and begin killing guests in the lobby area. The pair head upstairs, take hostages, and do as much damage to the hotel as possible with their grenades and IEDs. When these run out, they take to igniting mattresses. Both men die after a protracted game of cat and mouse with Indian commandos in the burning hotel.

Team 4: Abdul Rehman Chotta and Fahadullah enter the main entrance of the Oberoi-Trident Hotel, proceed to the hotel's restaurant, and attack diners there. They ignite two IEDs in the lobby and then head to the building's upper floors, firing as they go. They take hostages and are killed when NSG commandos raid the hotel.

Team 5: Babar Imran and Nazir throw grenades at a gasoline station, then force their way into a community center called the Chabad House that caters to Jews. The pair take hostages, some of which appear to have been tortured before they were killed. NSG commandos use helicopters to land on the center's roof. Imran and Nazir perish in the ensuing gun battle.

---

i. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008," Federation of American Scientists website: http://www.fas.org/irp/eprint/mumbai.pdf.

ii. Angel Rabasa et al., *The Lessons of Mumbai,* Santa Monica, CA: RAND Corporation, 2009. Available at http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf.

iii. New York Police Department Intelligence Division, "Mumbai Attack Analysis," December 4, 2008, http://publicintelligence.net/nypd-law-enforcement-sensitive-mumbai-attack-analysis/.

Unknown to the terrorists, the Indian government claimed that it had intercepted virtually all of the conversations between the attackers and their handlers back in Pakistan. Transcripts of the conversations that have been released detail how LeT commanders kept the teams in Mumbai informed about the movement of Indian security forces, offering advice such as "throw one or two grenades at the Navy and police teams, which are outside."[53] The commanders also reminded the teams that "everything is being recorded by the media" and that they needed to "inflict the maximum damage." When team members grew tired or frustrated, their leaders encouraged them to keep fighting. "Don't be taken alive," one of the voices from Pakistan instructed.

The Endgame

On the morning of 27 November, Indian commandos mounted an assault on the Oberoi Hotel and began room-to-room searches through the hotel's 877 units.[54] It was later revealed that at least 380 people were trapped in the hotel at the time of the attack.[55] Indian forces spent the rest of the day and part of the next morning freeing hostages and chasing down the two terrorists fortified inside the massive building.[56] When the operations concluded, both terrorists were dead.

The NSG employed a helicopter to land commandos on the roof of the Chabad House on the morning of 28 November.[57] "Brother you have to fight," a LeT commander told a militant inside during their final conversation. "This is a matter of the prestige of Islam."[58] The two gunmen managed to keep their Indian opponents at bay for almost twelve hours, despite the building's small size (in relation to the seized hotels).[59] Six people were killed inside the Chabad before the standoff was broken.[60]

The assault on the Taj Hotel began at about the same time as the operation at the Oberoi Hotel, but not until the morning of 29 November—nearly two and a half days later—was the landmark hotel secured.[61] The difficulty at the Taj Hotel was the number of guests—about 450 people, many of them hiding in their rooms—who needed to be located. The task was made all the more difficult by the numerous fires that raged inside the building (LeT attackers had been throwing grenades and igniting mattresses for several hours).[62, 63] "We were working in two teams, combing the hotel top to bottom" said Sunil Kumar, an NSG commando.[64] "We cleared the sixth floor and roof without incident. Then the fifth. Then the fourth. By the time we got to the third floor, it was too late. There were simply too many rooms. Many wouldn't open, even with the master

key. We had to enter by force to get people out who were too scared to evacuate."[65] As the commando teams crept through the smoke-filled hotel, hostages trapped upstairs unfurled banners that said "Save Us" from the windows of their rooms.[66] From Pakistan, the message from the LeT commanders was indisputable: "The hostages are of use only as long as you do not come under fire. If you are still threatened, then don't saddle yourself with the burden of the hostages. Immediately kill them."[67] A total of thirty-two people were killed in the hotel during the three-day ordeal before it was retaken by Indian forces.[68]

The Aftermath

More than 160 people died, and over 300 people sustained injuries during the 60-hour rampage.[69] In the wake of the attacks, Indian investigators quickly identified the attackers as Pakistani. It was not difficult to link the attackers to LeT once their nationality was established. By the time the investigation concluded, Indian officials alleged that elements within the Pakistani intelligence services had helped LeT with the assault—or, at the very least, had known about the attack and done nothing to prevent it. The government of Pakistan initially denied there was any connection between that country and the attack.[70] However, faced with hours of intercepted phone calls and a mountain of forensic evidence, Pakistani officials were ultimately forced to concede the assault was planned in their country and that the gunmen had trained in LeT camps located there. In 2009, Pakistan charged LeT's military chief and six less influential suspects in the Mumbai attacks and brought them to trial. US officials say, however, that the trial seems hopelessly stalled over legal complications and conflict with India.[71, 72]

Kasab, the only gunman who survived the attack, initially confessed to taking part in the attack, and he went on to provide a great deal of information about his recruitment in Pakistan, his training, and his fellow attackers.[73] He later changed his story in court and argued that he was a tourist who had been framed by the Mumbai police. Kasab was convicted of murder, damage to public property, and a host of other minor charges in May 2010. "It was not a simple act of murder," the presiding judge said of the attacks at the conclusion of Kasab's trial. "It was war."[74] Kasab was sentenced to death. More than thirty-eight other people, most of whom live in Pakistan, have been charged in connection to the attacks. LeT commander Rehman and at least nineteen others have been found guilty in absentia by Indian courts.

KEY TAKEAWAYS

- Predicting how a terrorist group might launch an attack is a daunting task. The best analyses consider the broadest range of credible alternatives and then narrow the list down to those that are most attention deserving.
- Structured Brainstorming provides a good method for ensuring that all possible options have been considered; its power is that it stimulates creative thinking. Classic Quadrant Crunching™ is a more rigorous and systematic process that usually generates a robust set of alternatives because it forces the analyst to think about the problem from a wide variety of very different optics.
- When generating a list of indicators to guide collection, analysts should focus their energies on developing truly diagnostic indicators that can drive the analysis and focus the attention of investigators on what really matters, especially when time is of the essence. Collectors usually prefer working with a short list of tailored indicators as opposed to a long list of all possible indicators that might be relevant.
- In a crisis environment, imprecise and often incorrect reporting is the norm, especially when relying on eyewitness reports. Always include with such information caveats as, for example, "initial reports."

INSTRUCTOR'S READING LIST

Government of India. *Mumbai Terrorist Attacks: Nov. 26–29, 2008*. Federation of American Scientists website: http://www.fas.org/irp/eprint/mumbai.pdf.

Haq, Noor ul (with Khalid Hussain), ed. *Mumbai Terrorist Attack*. Islamabad, Pakistan: Islamabad Policy Research Institute, 2009. Available at http://www.ipripak.org/factfiles/ff107.pdf.

New York Police Department Intelligence Division. "Mumbai Attack Analysis." December 4, 2008. http://publicintelligence.net/nypd-law-enforcement-sensitive-mumbai-attack-analysis.

Rabasa, Angel, et al. "The Lessons of Mumbai." Santa Monica, CA: RAND Corporation, 2009. Available at http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf.

Rotella, Sebastian. "On the Trail of a Terrorist." *Washington Post,* November 14, 2010.

Rotella, Sebastian. "On the Trail of the Mumbai Attackers: An Intricate Plot Unleashed, the West Confronts a New Threat." *Washington Post*, November 15, 2010.

Tankel, Stephen. *Storming the World Stage: The Story of Lašhkar-ĕ-Taiba*. London: Hurst, 2011

NOTES

1. The description of Red Hat Analysis in this case was taken from the first edition of Structured Analytic Techniques for Intelligence Analysis. A more robust approach for conducting Red Hat Analysis has subsequently been developed that appears in the second edition of the book but was not used in this case study.
2. Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis,* 2nd ed. (Washington, DC: CQ Press, 2015), 63.
3. Ibid., 209.
4. Ibid., 144.
5. Angel Rabasa et al., *The Lessons of Mumbai,* Santa Monica, CA: RAND Corporation, 2009. Available at http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf.
6. For a full explanation of Analysis of Competing Hypotheses, see *Structured Analytic Techniques for Intelligence Analysis,* 2nd ed. (Washington, DC: CQ Press, 2015), 181.
7. Sebastian Rotella, "On the Trail of a Terrorist," ProPublica, *Washington Post,* November 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/13/AR2010111304345.html.
8. Ibid.
9. Richard Esposito, Brian Ross, and Pierre Thomas, "US Warned India in October of Potential Terror Attack," *ABC World News,* December 1, 2008, http://abcnews.go.com/Blotter/story?id=6368013.
10. Rotella, "On the Trail of a Terrorist."
11. Pranab Dhal Samanta, "Mumbai Sea Attack Alert Came Nov. 19," *Indian Express,* November 30, 2008, http://www.indianexpress.com/news/mumbai-sea-attack-alert-came-nov-19/392351.
12. Rotella, "On the Trail of a Terrorist."
13. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008," Federation of American Scientists website: http://www.fas.org/irp/eprint/mumbai.pdf.
14. Rotella, "On the Trail of a Terrorist."
15. New York Police Department Intelligence Division, "Mumbai Attack Analysis," December 4, 2008, http://publicintelligence.net/nypd-law-enforcement-sensitive-mumbai-attack-analysis.
16. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
17. Ibid.
18. New York Police Department Intelligence Division, "Mumbai Attack Analysis."
19. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
20. Rabasa et al., *The Lessons of Mumbai*.
21. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
22. Ibid.
23. Ibid.
24. New York Police Department Intelligence Division, "Mumbai Attack Analysis."
25. "How Mumbai Attacks Unfolded," BBC News, November 30, 2008, http://news.bbc.co.uk/2/hi/south_asia/7757500.stm.
26. Ibid.
27. Rotella, "On the Trail of a Terrorist."
28. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
29. New York Police Department Intelligence Division, "Mumbai Attack Analysis."
30. Aaron O. Patrick, "Eyewitness Account: Chaos at the Leopold Café," *Wall Street Journal,* November 28, 2008, http://online.wsj.com/article/SB122788875924764393.html.
31. New York Police Department Intelligence Division, "Mumbai Attack Analysis."
32. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
33. "How Mumbai Attacks Unfolded," BBC News.
34. Gethin Chamberlain, "Gunmen's Blow-by-Blow Account of Mumbai Attack after Change of Plea," *Guardian* (London), July 20, 2009, http://www.guardian.co.uk/world/2009/jul/20/mumbai-terrorist-attacks-gunman-trial.
35. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
36. New York Police Department Intelligence Division, "Mumbai Attack Analysis."
37. Rajanish Kakade, "Mumbai Cop, Left for Dead, Rides with Gunmen," Associated Press, *FoxNews.com*, November 30, 2008, http://www.foxnews.com/wires/2008Nov30/0,4670,ASIndiaLeftforDead,00.html.
38. New York Police Department Intelligence Division, "Mumbai Attack Analysis."
39. Rabasa et al., *The Lessons of Mumbai*.
40. "How Mumbai Attacks Unfolded," BBC News.
41. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
42. Ben Leach, "Mumbai Attacks: Eyewitnesses Describe Horror of Terrorist Raids," *Telegraph* (London), November 27, 2008, http://www.telegraph.co.uk/news/worldnews/asia/india/3529976/Mumbai-attacks-Eyewitnesses-describe-horror-of-terrorist-raids-Bombay-India.html.
43. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
44. Ibid.
45. "Witnesses Tell of Mumbai Violence," BBC News, November 27, 2008, http://news.bbc.co.uk/2/hi/7751423.stm.
46. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
47. Alastair Gee, "Mumbai Terror Attacks: And Then They Came for the Jews," *Sunday Times* (London), November 1, 2009, http://www.timesonline.co.uk/tol/news/world/asia/article6896107.ece.
48. "Mumbai Operation Appears Nearly Over," CNN, November 28, 2008, http://articles.cnn.com/2008–11–28/world/india.attacks_1_national-security-guard-mumbai-oberoi.
49. Ibid.
50. Rabasa et al., *The Lessons of Mumbai*.
51. Somini Sengupta, "Dossier Gives Details of Mumbai Attacks," *New York Times*, January 6, 2009, http://nytimes.com/2009/01/07/world/asia/07india.html.
52. Rotella, "On the Trail of a Terrorist."
53. Sengupta, "Dossier Gives Details of Mumbai Attacks."
54. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
55. "Mumbai Attacks: Key Sites," BBC News, November 26, 2009, http://news.bbc.co.uk/2/hi/south_asia/7751876.stm.

56. Rabasa et al., *The Lessons of Mumbai*.
57. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
58. Sengupta, "Dossier Gives Details of Mumbai Attacks."
59. Rabasa et al., *The Lessons of Mumbai*.
60. "Mumbai Attacks: Key Sites," BBC News.
61. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
62. Rabasa et al., *The Lessons of Mumbai*.
63. Sengupta, "Dossier Gives Details of Mumbai Attacks."
64. "Mumbai Terror Attacks: Commando Describes Taj Mahal Siege," *Telegraph* (London), December 1, 2010, http://www.telegraph.co.uk/news/worldnews/asia/india/3537891/Mumbaiterror-attacks-Commando-describes-Taj-Mahal-siege.html.
65. Ibid.
66. Emily Wax, "Indian Commandos Battle Assailants," *Washington Post,* November 28, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/11/27/AR2008112701128.html.
67. Sengupta, "Dossier Gives Details of Mumbai Attacks."
68. Government of India, "Mumbai Terrorist Attacks: Nov. 26–29, 2008."
69. After extensive investigative work, journalist Sebastian Rotella ("On the Trail of a Terrorist") concluded that 166 people were killed and 308 wounded in the attack.
70. Rotella, "On the Trail of a Terrorist."
71. Ibid.
72. Ibid.
73. "Ajmal Kasab," *New York Times,* May 4, 2010, http://topics.nytimes.com/top/reference/timestopics/people/k/ajmal_kasab/index.html.
74. Rina Chandran, "Indian Court Convicts Mumbai Attack Gunman," Reuters, May 3, 2010, http://www.reuters.com/assets/print?aid=USTRE6420WU20100503.

Table 15.4 ▶ Case Snapshot: Iranian Meddling in Bahrain		
Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Starbursting	p. 113	Idea Generation
Morphological Analysis	p. 119	Idea Generation
Structured Brainstorming	p. 102	Idea Generation
Indicators	p. 149	Scenarios and Indicators

15 Iranian Meddling in Bahrain

Cases in Intelligence Analysis: Structured Analytic Techniques in Action

Instructor Materials

This case provides a framework for tackling problems when information is scarce. It highlights a common problem for intelligence analysts who have deep substantive expertise but are confronted with questions for which that expertise is necessary but insufficient to answer policy makers' questions. For analysts, there is a great temptation to start with what is known and then build a plausible analysis around that information. A much more robust approach, however, starts with the analytic questions that need to be answered, a full explication of the potential explanations, and a robust list of collectible indicators that can help differentiate among possible answers.

While much is known in this case about the history of the region, internecine fighting, claims, and counterclaims, there is no direct information in the case that would help analysts deliver judgments about the truth of the Bahraini claims, Iranian denials, or opposition counterclaims. Nevertheless, US interests in the region—not the least of which include force protection issues surrounding the stationing of the US Fifth Fleet in Manama Bay—make this an issue with high-level policy maker interest. In situations such as this, it is incumbent upon the analyst to identify not only what is known and unknown, but also to list all possible explanations and to construct a focused collection strategy to help rule out explanations as new information is collected in the future.

The following techniques guide analysts through a process that helps them identify key questions in the case using Starbursting; explore possible alternatives for the claims and counterclaims using Morphological Analysis; explicate the key dimensions of the problem using Structured Brainstorming; and create specific indicators that will help guide future collection and analysis using Indicators. Taken together, these techniques force divergent thinking to ensure that all angles of the problem have been actively considered.

TECHNIQUE 1: STARBURSTING

Starbursting is a form of structured brainstorming that helps to generate as many questions as possible. It is particularly useful in developing a research project, but it can also be helpful to elicit many questions and ideas about conventional wisdom. This process allows the analyst to consider the issue at hand from many different perspectives, thereby increasing the chances that the analyst may uncover a heretofore unconsidered question or new idea that will yield new analytic insights.

Using this technique, analysts can quickly determine what is known, what is knowable, and what will probably not be knowable in the foreseeable future. Even more important, it quickly helps identify the key questions to which additional resources should be devoted.

Task 1.

Starburst the Bahraini government claim that Bahraini elements are being trained in Iranian-backed Hezbollah camps specifically established to train assets from the Gulf in a plot to overthrow the monarchy.

Step 1: Use the template in Figure 15.1 in the book or draw a six-pointed star and write one of the following words at each point of the star: *Who, What, How, When, Where, Why.*

Step 2: Start the brainstorming session, using one of the words at a time to generate questions about the topic. Do

not try to answer the questions as they are identified; just focus on generating as many questions as possible. (See Figure 15.2.)

Step 3: After generating questions that start with each of the six words, the group should either prioritize the questions to be answered or sort the questions into logical categories.

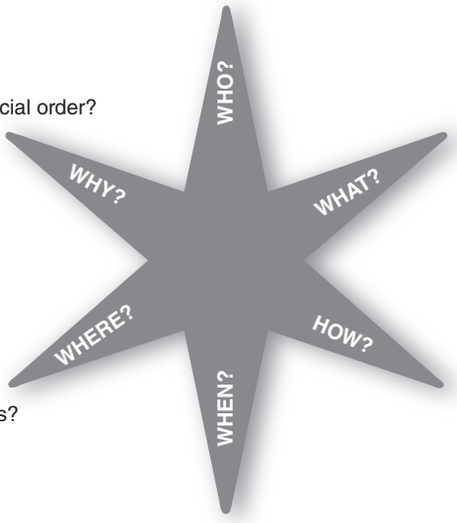
Analytic Value Added: As a result of your analysis, which questions or categories do you believe deserve further investigation? Are there any issues or questions in which your knowledge, based on the case, is particularly strong or deficient? Many of the questions are knowable in the Who, What, and When categories, such as who the Bahraini opposition figures are, what their chief complaints

Figure 15.2 ▶ Starbursting Bahrain Example

- Who are the main Bahraini opposition figures?
- Who are fringe opposition figures?
- Who has shown a proclivity toward Iran in the past?
- Who supports them financially, ideologically, administratively?
- Who are their role models/what provides their ideological inspiration?
- What biographical information do we have for the main leaders?
- Who are their mentors? (Professors, Religious Leaders, Academic Advisors, Spiritual)
- Who has specific titles? (Official/Unofficial)
- Who are their friends, enemies, aliases, family members?

- What are the main opposition groups?
- What communities are they influencing?
- What inspired them?
- What is their agenda?
- What languages do they speak?
- What have they said publicly about Iran and the opposition efforts in Bahrain?
- What has been said about them?

- Why are they prominent?
- Why are they trying to change the social order?
- Why are they feared?
- Why are they Shia?



- Where do they communicate ideas?
- Where do they live?
- Where have they lived?
- Where are the alleged training camps?
- Where have they been arrested?
- Where does their family live?
- Where do they "vacation"?
- Where do they travel?
- Where do they own property?
- Where do they work?
- Where do they bank?

- When did they get the attention of the government?
- When have they been arrested or detained?
- When have they traveled to Lebanon or Iran?
- When did they start becoming involved in their cause?

- How involved are they in the community?
- How are they perceived in the community?
- How often do they travel?
- How do they communicate their message? (examples: elections, sermons, Facebook)
- How do they conduct training?
- How do they raise money?
- How do they communicate with colleagues?
- How do they propose to realize their agenda?
- How do they view the following: Iran, US, West, Hezbollah?

are, and when they came to the attention of the Bahraini government. Some, however, are much more difficult to answer, such as where the alleged camps are, who has traveled there, and for what purpose. Equally important are questions about who funds them, how they are funded, and why in particular they are feared. The Starburst helps to identify the full range of questions, which can then be prioritized by analysts according to relevance, accessibility, or another criterion. The process of identifying questions for prioritization easily translates into a strategy that can be used by a single analyst or a group to tackle an issue more efficiently.

TECHNIQUE 2: MORPHOLOGICAL ANALYSIS

Morphological Analysis is a method for systematically dealing with complex, nonquantifiable problems for which little information is available. It is especially useful in identifying possible variations of a threat or the way a set of driving forces might interact in ambiguous or information-poor situations. Morphological Analysis works through two common principles of creativity techniques: decomposition and forced association. By breaking down the problem and reassembling the various alternative dimensions, it helps generate a comprehensive list of possible outcomes, including low-probability/high-impact and "nightmare" scenarios that could have adverse implications for policy makers. This process helps to identify credible alternatives. Analysts can develop collection strategies to tackle them and indicators to help them determine whether or not a scenario is unfolding.

Task 2.

Conduct a Morphological Analysis of the claims, counterclaims, and other possible explanations for events in the case.

Step 1: Define the set of dimensions in the case. For example, the main dimensions—Group, Activity, Method, and Impact—have already been identified in the confidential report by the Bahraini government and could be used to frame the analysis. (See Table 15.5 in the book.) The counterclaims by the Bahraini opposition and Iran could also serve as additional alternative expressions of the dimensions.

Step 2: Create additional dimensions as needed.

Step 3: Consider all the combinations of dimensions to create a list of possible alternative scenarios. (See Table 15.6.)

Identifying the main claims, counterclaims, and null hypothesis are easily accomplished by looking down the columns:

- Bahraini opposition members receiving clandestine training in Iranian-backed Hezbollah camps with the purpose of overthrowing the Khalifa monarchy.
- Bahraini opposition members receiving clandestine financial support with the purpose of overthrowing the Khalifa monarchy.
- Bahraini opposition members who are overtly campaigning for minority Shia rights but are receiving no support.
- No activity.

The table also helps identify several alternatives, including:

- Bahraini opposition members who are unwitting of financial support that is aimed at overthrowing the Khalifa monarchy.
- Equally interesting is the possibility that unaffiliated or rogue opposition members are receiving training in camps but the activity has no impact because the Bahraini elements lack the organizational structure

Table 15.6 ▶ Bahrain Morphological Analysis Example

Dimensions			
Group	Bahraini Opposition Members	Unaffiliated Opposition	No Activity
Activity	Receiving Training in Iranian-backed Hezbollah Camps	Financial Support	No Support
Method	Clandestine	Overt	Unwitting
Impact	Overthrow the Khalifa Monarchy	Obtain Greater Shia Minority Rights	No Impact

that would enable them to put the training into action once they return to Bahrain.

Step 4: Eliminate any combinations that are impossible, impractical, or undeserving of attention.

Nonsensical combinations should be discarded—for example, a scenario in which individuals receiving the training are unwitting of it.

Step 5: Refine the scenarios so that they are clear and concise.

- Bahraini opposition members are receiving clandestine training in Iranian-backed Hezbollah camps with the purpose of overthrowing the Khalifa monarchy.
- Bahraini opposition members are receiving clandestine financial support with the purpose of overthrowing the Khalifa monarchy.
- Bahraini opposition members who are overtly campaigning for minority Shia rights are receiving no Iranian support.
- Bahraini opposition members are receiving financial support with the purpose of overthrowing the Khalifa monarchy but are unwitting of the source of that funding.
- Unaffiliated or rogue opposition members are receiving clandestine training in camps that has not yet had an impact in Bahrain.

Analytic Value Added: Which scenarios are most deserving of attention? Do any assumptions underlie the scenarios? Certainly, the main claims and counterclaims deserve attention, but equally important in this case is the possibility that the opposition is unwitting that it is receiving support from Iran. In this scenario, there is a possibility that cooptation and influence by Iran are occurring, but the opposition is not yet aware of that activity. It also raises the possibility that only select individuals associated with otherwise legitimate Bahraini opposition groups may be aware of the activity while the larger organization is not.

Are there any information gaps that affect your ability to assess the likelihood of a scenario? Information is lacking about the locations of the alleged training camps, the individuals who have traveled there, or the specifics relating to alleged financial support such as bank accounts or amounts of transfers. These gaps limit our ability to assess the likelihood of several of the scenarios.

TECHNIQUE 3: STRUCTURED BRAINSTORMING

Brainstorming is a group process that follows specific rules and procedures designed for generating new ideas and concepts. The stimulus for creativity comes from two or more analysts bouncing ideas off each other. A brainstorming session usually exposes an analyst to a greater range of ideas and perspectives than the analyst could generate alone, and this broadening of views typically results in a better analytic product. (See Box 15.1 in the book.)

Structured Brainstorming is a more systematic twelve-step process for conducting group brainstorming. It requires a facilitator, in part because participants are not allowed to talk during the brainstorming session. Structured Brainstorming is most often used to identify key drivers or all the forces and factors that may come into play in a given situation.

Task 3.

Conduct a Structured Brainstorming exercise to identify all the factors that could help determine whether or not Bahraini opposition figures are being aided by the Iranian government.

Step 1: Gather a group of analysts with knowledge of the target and its operating culture and environment.

Step 2: Pass out sticky notes and marker-type pens to all participants. Inform the team that there is no talking during the sticky-notes portion of the brainstorming exercise.

Step 3: Present the team with the following question: Are Bahraini opposition groups being aided by the Iranian government?

Step 4: Ask them to conduct a Structured Brainstorming exercise to identify all the factors that could help determine whether or not Bahraini opposition figures are being aided by the Iranian government.

Step 5: Ask the group to write down responses to the question with a few key words that will fit on a sticky note. After a response is written down, the participant gives it to the facilitator, who then reads it out loud. Marker-type pens are used so that people can easily see what is written on the sticky notes when they are posted on the wall.

Step 6: Post all the sticky notes on a wall in the order in which they are called out. Treat all ideas the same.

Encourage participants to build on one another's ideas. Usually an initial spurt of ideas is followed by pauses as participants contemplate the question. After five or ten minutes there is often a long pause of a minute or so. This slowing down suggests that the group has "emptied the barrel of the obvious" and is now on the verge of coming up with some fresh insights and ideas. Do not talk during this pause, even if the silence is uncomfortable.

Step 7: After two or three long pauses, conclude this divergent-thinking phase of the brainstorming session.

A list of brainstorming results appears in Figure 15.3

Step 8: Ask all participants (or a small group) to go up to the wall and rearrange the sticky notes by affinity groups (groups that have some common characteristics). Some sticky notes may be moved several times; some may also be copied if an idea applies to more than one affinity group.

Step 9: When all sticky notes have been arranged, ask the group to select a word or phrase that best describes each grouping.

See Figure 15.4 for an example of affinity-clustered results.

Step 10: Look for sticky notes that do not fit neatly into any of the groups. Consider whether such an outlier is useless noise or the germ of an idea that deserves further attention.

Step 11: Assess what the group has accomplished. What are the main dimensions that the group has identified?

Use this opportunity to refine the clusters. Take a step back and ask what the main emphasis of the cluster is. For example, family, financial, or professional problems might reflect vulnerabilities to recruitment.

Step 12: Present the results, describing the key themes or dimensions of the problem that were identified.

Analytic Value Added: What affinity clusters emerged? What are the key dimensions of the problem? The main affinity clusters were Family, Outside Influences, Malleable Personal Ideas, Vulnerability, Opportunity to Be Influenced, and Foreign Actors. Upon subsequent

Figure 15.3 ▶ Bahrain List of Brainstormed Ideas

Love/Marriage	Foreign Media	Iranian Regime
Marriage/Relationships	Vulnerability	Iran
Personal Attributes	Money Needs	History of Employment
Language Spoken	Green Revolution	Unemployment
Age	Neda	Criminal Record
Ethnicity	Malleable Personal Ideas	Connection to Organized Crime
Religion	Beliefs	Narcotic Use/Distribution
Intelligence	Personal Goals	Public Statements against the West
Mentor(s)	Values	Degree of Organization
Associates	Need for Adventure	Administrative Savvy
Wealth	Need for Attention	TV Shows/Foreign Media
Ownership in Bahrain	Anger	Chance
Ownership in Iran	Injustice	How Often They Travel to Iran?
Location	Education	Travel
Social Affiliations	Religious Education	Accounting
Ties to the West	Social Background	Children
Support in West	Discontent	Family History
TV Shows	Skill of Iranian Officers	Family Ties
Contacts in Foreign Countries	Iranian Aggressiveness	

Figure 15.4 ▶ Bahrain Affinity Clusters

Family
Love/Marriage
Children
Family History
Family Ties
Marriage/Relationships
Personal Attributes
Language Spoken
Age
Ethnicity
Religion
Intelligence

Outside Influences
Mentor(s)
Associates
Education
Religious Education
Social Affiliations
Ties to the West
Support in West
TV Shows
Foreign Media
Green Revolution

Malleable Personal Ideas
Beliefs
Personal Goals
Values
Need for Adventure
Vulnerabilities
Need for Attention
Anger
Injustice
Discontent

Vulnerability
Money Needs
History of Employment
Social Background
Wealth
Ownership in Bahrain
Ownership in Iran
Criminal Record
Connection to Organized Crime
Narcotic Use/Distribution
Public Statements against the West

Opportunity to Be Influenced
Degree of Organization
Administrative Savvy
TV Shows/Foreign Media
Chance
How Often They Travel to Iran?
Travel
Accounting
Contacts in Foreign Countries

Foreign Actors
Skill of Iranian Officers
Iranian Aggressiveness
Iranian Regime
Iran

refinement, it becomes apparent that the clusters center on the presence or absence of:

- Vulnerabilities
- Pro-Iranian influences
- Pro-Iranian beliefs
- Opportunities for cooptation

These dimensions of the problem clearly focus on factors that could help determine whether or not Bahraini opposition figures are being aided by the Iranian government.

TECHNIQUE 4: INDICATORS

Indicators are observable or deduced phenomena that can be periodically reviewed to track events, anticipate an adversary's plan of attack, spot emerging trends, distinguish among competing hypotheses, and warn of unanticipated change. An indicators list is a preestablished set of actions, conditions, facts, or events whose simultaneous occurrence would argue strongly that a phenomenon is present or about to be present or that a hypothesis is correct. The identification and monitoring of indicators are fundamental tasks of intelligence analysis, as they are the principal means of avoiding surprise. In the law enforcement community, indicators are used to assess whether a target's activities or behavior are consistent with an established pattern or lead hypothesis. These are often described as descriptive indicators that look backward. In intelligence analysis, indicators are often described as predictive indicators that look forward.

Preparation of a detailed indicator list by a group of knowledgeable analysts is usually a good learning experience for all participants. It can be a useful medium for an exchange of knowledge between analysts from different organizations or those with different types of expertise—for example, counterterrorism or counter drug analysis, infrastructure protection, and country expertise. The indicator list can become the basis for conducting an investigation or directing collection efforts and routing relevant information to all interested parties. Identification and monitoring

of indicators or signposts that a scenario is emerging can provide early warning of the direction in which the future is heading, but these early signs are not obvious. The human mind tends to see what it expects to see and to overlook the unexpected. Indicators take on meaning only in the context of a specific scenario with which they have been identified. The prior identification of a scenario and associated indicators can create an awareness that prepares the mind to recognize and prevent a bad scenario from unfolding or help a good scenario to come about.

In this exercise, instructors should encourage students to think creatively about how to get information. In a highly digital society, how might Bahraini opposition members use social media to gather information? What social media indicators might help analysts? What kind of information might be found there on associations, travel, interests, familial ties, or education, for example?

Task 4.

Using the Structured Brainstorming results to prompt your thinking, create tailored indicators for each of the main scenarios developed in Task 2: Morphological Analysis.

In the example below, we have focused on social media indicators due to space constraints and the fact that the Bahraini government and opposition members have actively used social media to organize and monitor recent protest activities in Bahrain.

Step 1: Create a list of the most attention-deserving scenarios to track for this case.

For this example, we will use three scenarios generated from the Morphological Analysis in Task 2:

- Bahraini opposition members are campaigning overtly for minority Shia rights and are receiving no Iranian support.
- Bahraini opposition members are receiving financial support with the purpose of overthrowing the Khalifa monarchy but are unwitting of the source of that funding.
- Bahraini opposition members are receiving clandestine training in Iranian-backed Hezbollah camps with the purpose of overthrowing the Khalifa monarchy.

Step 2: Work alone, or preferably with a small group, to brainstorm a list of indicators for each scenario.

Use the dimensions developed in Task 3 to prompt thinking.

Step 3: Review and refine each set of indicators, discarding any that are duplicative and combining those that are similar.

Step 4: Examine each indicator to determine whether it meets the following five criteria. Discard those that are found wanting.

1. **Observable and collectible.** There must be some reasonable expectation that, if present, the indicator will be observed and reported by a reliable source. If an indicator is to monitor change over time, it must be collectible over time.
2. **Valid.** An indicator must be clearly relevant to the endstate the analyst is trying to predict or assess, and it must be inconsistent with all or at least some of the alternative explanations or outcomes. It must accurately measure the concept or phenomenon at issue.
3. **Reliable.** Data collection must be consistent when comparable methods are used. Those observing and collecting data must observe the same things. Reliability requires precise definition of the indicators.
4. **Stable.** An indicator must be useful over time to allow comparisons and to track events. Ideally, the indicator should be observable early in the evolution of a development so that analysts and decision makers have time to react accordingly.
5. **Unique.** An indicator should measure only one thing and, in combination with other indicators, should point only to the phenomenon being studied. Valuable indicators are those that not only are consistent with a specified scenario or hypothesis but also are inconsistent with all other alternative scenarios.

Scenario 1: Bahraini opposition members are campaigning overtly for minority Shia rights and are receiving no Iranian support.

In this scenario, the indicators center on the lack of vulnerabilities, influences, beliefs, or opportunities that would facilitate cooptation by Iran. For example, there would be few or no apparent marital, family, money, professional, or criminal problems, and no Iranian-related influences or beliefs that would create an opportunity for Iran to influence, or coopt, the target. One potential pitfall in situations such as these is the failure to consider deceptive practices. For example, the absence of activities may be the result of operational security or a specific effort to conceal the activity. As a result, it is necessary to note the absence of activity across the dimensions of the problem and over time.

- No demonstrated marital or familial problems
- No resumed progression indicating professional problems
- No inconsistency between education/training and job
- No inconsistency between social media pictures showing standard of living and reported income
- No inconsistency between geographic location of home and reported income
- No business problems highlighted by public records data
- No articles or social media data on arrests, criminality, or drug or alcohol abuse
- No articles or social media data on perceived injustices toward person of interest or family
- Social media information reflecting marital harmony
- Articles or social media data illustrating sound finances
- Articles or social media data indicating close-knit family
- Resumed progression indicating professional success
- Articles/social media data indicating drug/alcohol abstinence
- Articles/social media data indicating history of lawfulness
- No pro-Iranian content in social media postings or published articles by mentors, professional associates, or friends
- Articles or social media data indicating that numerous friends or immediate family members live in the United States or Europe
- No articles/social media postings that include favorable citations of pro-Iranian TV/movies/books
- Visits to United States or from Americans/Europeans
- Descriptions in articles or social media of anti-Iranian influences
- No articles or social media postings indicating support for transnational Shiism
- Presence of articles or social media postings indicating transparency of lifestyle or personal conduct
- No public expressions of desire to travel to/live in Iran
- No favorable expressed opinions on Khomenei
- No favorable expressed opinions on Hezbollah
- No membership in Iranian-backed opposition group
- No favorable expressed opinions on Iranian Revolution
- Presence of favorable expressed opinions on United States/West
- No favorable expressed opinions on Syrian regime
- No suspected ethnic Persian names in social network
- No indications in articles/social media of travel to Iran
- No indications in articles/social media of travel to Europe, Asia, or Africa
- No indications from organization's website data of large number of employees, branches, or international presence
- Resumed data indicating training in accounting
- Resumed data indicating successful experiences managing large organizations
- Presence of social media picture postings with geocoordinates from foreign locations

Scenario 2: Bahraini opposition members are receiving financial support with the purpose of overthrowing the Khalifa monarchy but are unwitting of the source of that funding.

In this scenario, the indicators focus on financial connections between individual opposition members and their affiliated groups or parties and any Iranian-linked organizations or individuals. These may be hidden. The presence of pro-Iranian beliefs or significant personal vulnerabilities may or may not be present in this scenario.

- Publicly available financial information that links to shell or front companies in third countries
- Unexplained influx of donations from dubious sources
- Presence of suspected ethnic Persian names in social networks
- Presence of Iranian-connected organizations or individuals on opposition group advisory boards or social networks
- Indications from organization's website data of large number of employees, branches, or international presence

- No resumed data indicating training in accounting
- Little or no resumed data indicating successful experiences managing large organizations
- Inconsistency between social media pictures showing standard of living and reported income
- Inconsistency between geographic location of home and reported income
- Presence of public records data indicating business problems
- Presence of articles or social media data on arrests, criminality, or drug or alcohol abuse
- Some pro-Iranian content in social media postings or published articles by mentors, professional associates, or friends

Scenario 3: Bahraini opposition members are receiving clandestine training in Iranian-backed Hezbollah camps with the purpose of overthrowing the Khalifa monarchy.

In this scenario, multiple vulnerabilities are present and are compounded by more significant pro-Iranian influences and beliefs developed over time through contact with Iranian sympathizers or associates. Direct contacts with Iran may also be observed.

- Social media references to marital or familial problems
- Resumed progression indicating professional problems
- Inconsistency between education/training and job
- Inconsistency between social media pictures showing standard of living and reported income
- Inconsistency between geographic location of home and reported income
- Presence of public records data indicating business problems
- Presence of articles or social media data on arrests, criminality, or drug or alcohol abuse
- Presence of articles or social media data on perceived injustices toward POI or family
- No private chats demonstrating marital harmony
- No articles or social media data illustrating sound finances
- No articles or social media data indicating close-knit family
- Evidence of personal trauma (loss of family member, for example)
- Some pro-Iranian content in social media postings or published articles by mentors, professional associates, or friends
- Little or no presence of articles or social media indicating that numerous friends or immediate family members are living in the United States or Europe
- Some articles/social media postings that include favorable citations of pro-Iranian TV/movies/books
- No or little evidence of frequent visits to United States or from United States/Europe
- Few or no descriptions in articles or social media of pro-Western influences
- Some descriptions in articles or social media of pro-Iranian influences
- Articles or social media postings indicating support for transnational Shiism
- No articles or social media postings indicating transparency of lifestyle or personal conduct
- Public expressions of desire to travel to/live in Iran
- Favorable expressed opinions on Khomenei
- Favorable expressed opinions on Hezbollah
- Unfavorable expressed opinions on Green Revolution
- Membership in Iranian-backed opposition group
- Favorable expressed opinions on Iranian Revolution
- No favorable expressed opinions on United States/West
- Favorable expressed opinions on Syrian regime
- Descriptions in articles or social media of anti-Western views
- Descriptions in articles or social media of pro-Iranian views
- Presence of suspected ethnic Persian names in social network
- Indications in articles/social media of travel to Iran or Hezbollah
- Indications in articles/social media of travel to Europe, Asia, or Africa
- Possible indications from organization's website data of large number of employees, branches, or international presence
- Social media picture postings with geocoordinates from foreign locations

Analytic Value Added: Are the indicators mutually exclusive and comprehensive? Have a sufficient number of high-quality indicators been generated for each scenario to enable an effective analysis? Are the indicators collectible, and if so, what should be the collection priorities? The indicators in this case were generated on the basis of the dimensions developed in Task 3, and therefore reflect the range of issues identified in the divergent phase of Structured Brainstorming. This has resulted in a high number of indicators per dimension that analysts can reasonably expect to collect. The collection priorities for this case should focus on using the indicator sets to rule out the possibility that opposition members are engaged in activities to overthrow the Khalifa regime, rather than ruling in activity. Once the list has been narrowed, additional analysis and collection can be conducted to review thoroughly the basis for judgments about activities consistent with one or more of the scenarios. Some of the most interesting indicators surround the financial dealings of the opposition groups and members, their social networks, and the content and quality of their social media activities.

CONCLUSION

The standoff between the government and opposition did not abate in the months following the arrest of the eight opposition leaders. In June 2011, King Hamad sought to deescalate tensions by creating the Bahrain Independent Commission of Inquiry (BICI). The five-person commission's mandate was to determine whether the events of February and March 2011 involved violations of international human rights laws and norms and to make recommendations to the government.[1] In a 500-page report released in November 2011, the commission detailed government abuses and offered recommendations, some of which the government took steps to implement.[2] The commission found that "force and firearms were used in an excessive manner that was, on many occasions, unnecessary, disproportionate, and indiscriminate."[3] The report also documented 35 deaths, 559 allegations of torture, and 1,624 complaints of employment termination as a result of the uprising in Bahrain.[4] By early 2012, several of the board's recommendations had been implemented, including compensating families of deceased protestors and victims of torture, reviewing convictions, and promising to investigate allegations of torture.[5] On 8 January 2012, Bahrain's cabinet proposed granting more power to the elected legislature in order to "achieve greater balance between the executive and the legislative," but no effort was made to increase Shia representation in the political sphere.[6]

In addition to general recommendations to establish more independent institutions to investigate and oversee current and future claims of abuses, the commission offered specific recommendations to address the following:

- The use of force, arrest, treatment of persons in custody, detention, and prosecution in connection with the freedom of expression, assembly, and association.
- Demolition of religious structures, termination of employees of public and private sectors, dismissal of students, and termination of their scholarships.
- Media incitement issues.
- Better understanding and appreciation of human rights, including respect for religious and ethnic diversities.[7]

In many respects, however, the commission's recommendations and the government's response were too little and too late. For example, the government instituted a new code of conduct calling on police to be respectful of human rights principles; however, the government's detention of hundreds of opposition members in the months preceding and following the commission's report only fueled opposition calls for reforms and sparked additional protests that were met with government force.[8] In addition, the arrest and sentencing of forty-eight Bahraini doctors and nurses to five to fifteen years in prison for treating injured protestors fanned the flames of dissent and elicited stern rebukes from international institutions.[9] UN Secretary General Ban Ki-Moon, through his spokesperson, expressed his "deep concern over the harsh sentences handed down in Bahrain to civilians—medical professionals, teachers and others—by the Bahraini military Court of National Safety," pointing out that "proceedings were conducted under conditions that raised serious questions of due process irregularities."[10] In the months following the report, clashes between police and protesters continued, prompting the Office of the U.N. High Commissioner for Human Rights to issue a statement on "worrying reports" about the use of tear gas, rubber bullets, and birdshot pellets. The OHCHR said "reliable sources" indicated that a number of deaths were linked to the use of tear gas fired by security forces into crowds and called on the government of Bahrain to investigate the alleged use of such excessive force.[11]

Bahraini–Iranian relations cooled further in the wake of the protests. The Bahraini government, in its official capacity and through unofficial forums and social networking sites, accused almost every opposition leader of being influenced by or connected to Iran. It also accused international human rights organizations that had voiced support for the opposition movement of collusion with Iran. Both sides withdrew their ambassadors in 2011.

Whether or not any of the 14 February protesters had links to Iran or received training and support via Hezbollah, however, remains an unanswered question. The Bahraini government publicly offered no evidence of direct Iranian meddling or support to the arrested opposition activists, and the opposition leaders remained in detention through 2011. In November 2011, Bahrain issued new accusations, stating that it had arrested five members of an underground terrorist cell with direct links to the Iranian Revolutionary Guard Corps who were plotting to attack Bahraini government buildings and the causeway linking Bahrain to Saudi Arabia.[12] Bahrain released neither the names nor any evidence proving the alleged links, and protests continued well into 2012 unabated.

KEY TAKEAWAYS

- In the absence of direct reporting, use divergent techniques such as Starbursting and Structured Brainstorming to develop a robust set of questions and issues for research.
- Indicators help focus research on relevant, collectible information that can be used to focus collection and mitigate the human tendency to see what one expects to see and to overlook the unexpected.

NOTES

1. Report of the Bahrain Independent Commission of Inquiry, November 23, 2011, http://www.bici.org.bh.
2. "Background Note: Bahrain," U.S. State Department Bureau of Near Eastern Affairs, January 13, 2012, http://www.state.gov/r/pa/ei/bgn/26414.htm.
3. Report of the Bahrain Independent Commission of Inquiry, 268.
4. Ibid., 219, 282, 331.
5. Information Affairs Authority, "Progress Report on the Implementation of the BICI Recommendations," January 17, 2012.
6. Report of the Bahrain Independent Commission of Inquiry.
7. Ibid.
8. "Post BICI Report: A BCHR Report on Human Rights Violations Since the BICI Report," Bahrain Centre for Human Rights, March 26, 2012, http://bahrainrights.hopto.org/BCHR/wp-content/uploads/2012/03/PostBICIreview-1.pdf.
9. "Re-trial for Bahrain Medics Important Step Towards Justice," Amnesty International, October 6, 2011, http://www.amnesty.org/en/news-and-updates/re-trial-bahraini-medics-'important-step-towards-justice'-2011-10-06.
10. "UN Condemns 'Harsh' Bahrain Sentencing," RTE, October 1, 2011, http://www.rte.ie/news/2011/1001/bahrain.html.
11. "U.N. Concerned by Bahrain's Crackdown," UPI, March 20, 2012, http://www.upi.com/Top_News/Special/2012/03/20/UN-concerned-by-Bahrains-crackdown/UPI-92081332265828.
12. "Bahrain Says Terror Suspects Linked to Iran's Revolutionary Guard," *The Guardian*, November 14, 2011, http://www.guardian.co.uk/world/2011/nov/14/bahrain-terror-iran-revolutionary-guard.

Table 16.1 ▶ Case Snapshot: Shades of Orange in Ukraine		
Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Structured Brainstorming	p. 102	Idea Generation
Outside-In Thinking	p. 228	Assessment of Cause and Effect
Simple Scenarios	p. 139	Scenarios and Indicators

16 Shades of Orange in Ukraine
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

One of the most important ways that analysts can help policy makers prepare for uncertain future outcomes is to identify the key factors at play and explain their dynamics. It is sometimes tempting to offer predictions about how a situation will turn out, but single-point forecasts of distant outcomes are nearly always incorrect and seldom are relevant to the considerations required for sound policy decisions. Effective foreign and security policy must be applicable to a range of possible outcomes, and policy makers need a good sense of which factors they can influence as they attempt to maximize the chances that events will conform to the nation's interests. Moreover, they must consider the potential "opportunity costs" of policy options—the impact that a given approach to one situation might have on an important goal in another policy area.

In this case, students face the temptation to focus their analysis on which candidate is most likely to win the presidential election. The case narrative concentrates largely on domestic developments in Ukraine, as it is designed to simulate the focus of analysts responsible for understanding the country's internal politics. Such a focus can come at the expense of identifying critical external factors, however. Box 16.2 on Russia and Box 16.3 on Georgia in the case provide clues about the kinds of external factors that could affect the outcome of the election. The Structured Brainstorming, Outside-In Thinking, and Simple Scenarios techniques help analysts overcome the temptation to offer single-point electoral predictions or focus on too narrow a set of driving factors. Taken together, they frame an analytic process that can identify all relevant factors—direct and indirect, external and internal—and aid in understanding the interrelationships among them. Instructors should encourage analysts to consider carefully the process by which they complete the tasks in these exercises, because it is applicable to many analytic support situations.

TECHNIQUES 1 & 2: STRUCTURED BRAINSTORMING AND OUTSIDE-IN THINKING

Brainstorming is a group process that follows specific rules and procedures designed for generating new ideas and concepts (see Box 16.4). The stimulus for creativity comes from two or more analysts bouncing ideas off each other. A brainstorming session usually exposes an analyst to a greater range of ideas and perspectives than the analyst could generate alone, and this broadening of views typically results in a better analytic product.

Outside-In Thinking helps analysts who are familiar with issues related to their own fields of specialization consider how factors external to their areas of expertise could affect their analyses. This technique is most helpful when considering all the factors at play at the beginning of an analytic process. Outside-In Thinking can reduce the risk of analytic failure by helping analysts identify external factors and uncover new interrelationships and insights that otherwise would be overlooked.

Using these two techniques together prompts analysts to consider the full range of factors that could shape the outcome of the election.

Box 16.4 EIGHT RULES FOR SUCCESSFUL BRAINSTORMING

1. Be specific about the purpose and the topic of the brainstorming session.
2. Never criticize an idea, no matter how weird, unconventional, or improbable it might sound. Instead, try to figure out how the idea might be applied to the task at hand.
3. Allow only one conversation at a time and ensure that everyone has an opportunity to speak.
4. Allocate enough time to complete the brainstorming session.
5. Engage all participants in the discussion; sometimes this might require "silent brainstorming" techniques such as asking everyone to be quiet for five minutes and write down their key ideas on 3 × 5 cards and then discussing what everyone wrote down on their cards.
6. Try to include one or more "outsiders" in the group to avoid groupthink and stimulate divergent thinking. Recruit astute thinkers who do not share the same body of knowledge or perspective as other group members but have some familiarity with the topic.
7. Write it down! Track the discussion by using a whiteboard, an easel, or sticky notes.
8. Summarize key findings at the end of the session. Ask the participants to write down their key takeaways or the most important things they learned on 3 × 5 cards as they depart the session. Then, prepare a short summary and distribute the list to the participants (who may add items to the list) and to others interested in the topic (including those who could not attend).

Task 1.

Conduct a Structured Brainstorming of the factors that will determine the outcome of the Ukrainian election.

Step 1: Pass out sticky notes and marker-type pens to all participants. Inform the team that there will be no talking during the sticky-notes portion of the brainstorming exercise.

Students will be limited to the case study for this exercise, but it is important to point out that in real-life situations, it is helpful to include in the brainstorming group both experts on the topic and generalists who can provide more diverse perspectives. When only those working the issue are included, often the group's perspective is limited to the stream of reporting it reads every day; as a result, key assumptions remain unchallenged, and historical analogies can be ignored.

Step 2: Display the following focal question for the team: What are all the factors that will determine who will be the next Ukrainian president?

Step 3: Ask the group to respond to the question by writing a few key words on their sticky notes. After a response is written down, the participant gives it to the facilitator, who then reads it out loud. Marker-type pens are used so that people can easily see what is written on the sticky notes when they are posted on the wall. Urge participants to use short phrases rather than long sentences.

Step 4: Post all the sticky notes on a wall in the order in which they are called out. Treat all ideas the same. Encourage participants to build on one another's ideas. Usually there is an initial spurt of ideas followed by pauses as participants contemplate the question.

It is important to emphasize the importance of avoiding mirror imaging. In a classroom situation, many students may not know much about the Ukrainian political landscape; this is why it is important to ensure that all participants read the case study with the relevant background material carefully. They should have the case study at hand for quick reference.

By using the case narrative, students should quickly identify the internal political factors that will most likely shape the election landscape. These include the most likely candidates and their bases of support and the election environment, including media freedom and role of nongovernmental organizations (NGOs) working in the country.

Step 5: After five or ten minutes there is often a long pause of a minute or so. This slowing down suggests that the group has "emptied the barrel of the obvious" and is now on the verge of coming up with some fresh insights and ideas. Do not talk during this pause, even if the silence is uncomfortable.

Step 6: After two or three long pauses, encourage Outside-In Thinking by asking the group specifically to focus on identifying external factors that could affect the outcome of the Ukrainian election. Use the mnemonic STEEP +2 (Social, Technological, Economic, Environmental, Political, plus Military and Psychological) to catalyze the process.

During this phase, students should begin to note the potential role of the United States, European Union (EU), Russia, international institutions such as the Organization for Security and Cooperation in Europe (OSCE), and foreign NGOs. In addition, the use of STEEP +2 should elicit factors such as the roles nontraditional media, cell phones, and social media sites may play in sharing information and rallying support. During this phase students might note the Rose Revolution in Georgia, the psychological impact that this event might have on Ukrainians, and the possibility of links between the opposition in both countries.

Give the students a few minutes of brainstorming and pauses to think about the issue and jot down a few ideas. Then go around the room and collect the sticky notes. Read the responses slowly and post them on the wall or the whiteboard in random order as you read them. A list of brainstorming results appears in Figure 16.3.

Step 7: Ask all participants (or a small group) to go up to the wall and rearrange the sticky notes by affinity groups (groups that have some common characteristics). Some sticky notes may be moved several times; some may also be copied if an idea applies to more than one affinity group.

If only a subset of the group goes to the wall to rearrange the sticky notes, then ask those who are remaining in their seats to form small groups and come up with a list of key drivers or dimensions of the problem based on the themes they heard emerge when the instructor read out the sticky notes. This keeps everyone busy and provides a useful check on what is generated by those working at the whiteboard.

Step 8: When all sticky notes have been arranged, ask the group to select a word or phrase that best describes each grouping.

Figure 16.3 ▶ Ukraine Brainstorming Results Example

- Ukrainian economy
- Yushchenko's ability to galvanize support
- Yushchenko
- Media
- Media coverage
- "New" media
- Demonstrations á la Rose Revolution
- NGOs
- Russian "meddling"
- State of Ukraine's economy and Russia's ability to influence it
- Tymoshenko's bloc aligned with Yushchenko
- Symonenko
- Medvedchuk maneuvering
- State-controlled media
- Effectiveness of election monitoring
- Political demography
- Additional compromising information about Kuchma or Yanukovych
- New constitutional reform bill
- US support for NGOs
- Energy interests
- Demographic distribution
- Popular attitudes toward government
- Likelihood of fraud
- Degree to which playing field is level
- State of media freedom
- Campaign resources (business support?)
- Role of Russian involvement
- Degree and nature of European involvement
- Degree and nature of US involvement
- Role of Ukrainian and foreign NGOs
- Role of external official institutions like OSCE, Council of Europe
- Psychological impact of Rose Revolution
- Role of technology
- Likelihood of a coup
- Likelihood of debilitating violence against one or both of the leading candidates
- Role of organized crime
- Prospects for NATO and EU enlargement and membership for Ukraine

See Figure 16.4 for an example of affinity-clustered results.

Only two clusters are shown in Figure 16.4, but four or five themes usually emerge from this part of the exercise. In this case, a notional set of groups might include the following:

- Leonid Kuchma's maneuvering.
- Expected candidates and their bases of support (Viktor Yushchenko, Viktor Yanukovych).
- Role of the media.
- Russian influence.
- US/EU/Western influence.
- Business interests.
- Nongovernmental organizations.
- Popular sentiment.

Step 9: Assess specifically how each of these forces and factors could have an effect on the problem and, using this list of forces and factors, generate a list of areas for additional collection and research.

Kuchma's maneuvering: Kuchma is taking steps to alter the constitution to deprive the new president of significant powers. Kuchma has been accused in the past of unscrupulous dealings, raising questions about just how far he will go to ensure Yanukovych's victory and how effective he might be in doing so. Would he try to prolong his own rule by provoking a crisis? Would he take ruthless steps to silence the opposition? Or would he attempt to divide the opposition by wooing one or more of its significant members away from Yushchenko's camp?

Expected candidates and their bases of support: How the candidates conduct their campaigns, including their ability to garner support from voters and business leaders, will affect voter turnout and financial support. The degree of corruption and fraud are key unknowns.

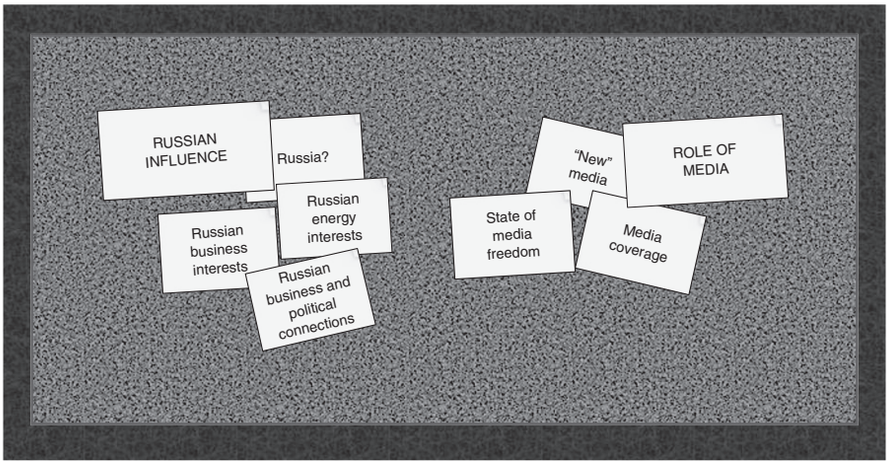
Role of the media: The media are largely controlled by the government in Ukraine and present few, if any, opposing political viewpoints. The opposition at their February convention showed a creative use of technology and nontraditional media to broadcast their message. Also, there is an underlying assumption that control of the media will only help the incumbent, when it is possible that the lack of alternative perspectives could encourage an engaged electorate to seek out nontraditional sources of information. A gap that additional research could fill is the extent to which the opposition is tapping other forms of communication and, if it is, what these forms of communications are.

Russian influence: The case narrative highlights strong motivations to discourage a Yushchenko presidency, but the case does not identify specifically Russia's potential means for influencing a transition. Russia's means of influencing the outcome and indications that Moscow is exercising those means are an avenue for further research. If Russia sees Ukraine as its most important foreign policy issue, how far will it go to protect its interests in Ukraine?

US/EU/Western influence: The United States and other Western countries, including international organizations, have provided aid—via foreign NGOs and international institutions such as the Council of Europe, the OSCE, etc.—to fledging civil society organizations in other countries. To what extent are they funding these organizations in Ukraine and to what effect?

Business interests: Ukrainian businesspeople are in a position to influence the election by providing financial support to the candidates and enabling access to the media. Some businesspeople have withdrawn their support

Figure 16.4 ▶ Ukraine Brainstorming Affinity Cluster Examples



for Yanukovych and are backing Yushchenko. Which businesspeople are supporting the main candidates, how strong is their support, and how might their support tip the balance in one direction or the other?

Nongovernmental organizations: NGOs are operating in Ukraine. To what extent can NGOs organize the kinds of activities that took place in Georgia's Rose Revolution? To what extent is Kuchma taking preemptive action to prevent such activities?

Popular sentiment: How does the Ukrainian electorate perceive the candidates and the contest in general? What are their perceptions of Western or Russian involvement? And what will be their level of voter turnout and activism?

Analytic Value Added: What key factors will influence the outcome of the election? What gaps deserve additional attention? The value added by this combination of Structured Brainstorming and Outside-In Thinking is not only the list of driving factors but also a clear exposition of why the factors could influence the outcome and how additional collection can narrow the range of uncertainty by filling important information gaps. This process can focus information collection tasks on the most meaningful and potentially fruitful avenues of inquiry because analysts have focused on factors that they have reason to suspect will influence the outcome and the specific information needs surrounding them. Some gaps are knowable, and information can be collected. Some of them are not knowable, but the mere act of considering them helps analysts identify the variables at play and place bounds around their uncertainty.

TECHNIQUE 3: SIMPLE SCENARIOS

The Simple Scenarios technique helps analysts develop an understanding of the multiple ways in which a situation might evolve. The technique can be used by an individual analyst or a group of analysts. In either situation, the analytic value added of Simple Scenarios lies not in the specifics of the scenarios themselves but in the analytic discussion of which drivers will affect a particular scenario, the implications of each scenario for policy makers, and the indicators that will alert policy makers to the fact that such a future is unfolding.

In this case, the simple act of creating multiple scenarios for how the situation will unfold forces the analyst to move away from "calling" the winner of the election and instead consider how the drivers can vary to produce radically different results.

Task 2.

Conduct a Simple Scenarios analysis to consider the range of possible outcomes and driving factors that will shape the outcome of the Ukrainian election.

Step 1: Clearly define the focal issue and the specific goals of the Simple Scenarios exercise.

In this case, the task above defines the focal issue, but students may want to consider whether any other focal issues warrant further consideration.

Step 2: Make a list of forces, factors, and events that are likely to influence the future.

Students can draw from the list of factors developed using Techniques 1 and 2 or brainstorm a list of factors that would have some effect on the issue being studied.

Step 3: Organize the forces, factors, and events that are related to each other into five to ten affinity groups that are expected to be the driving forces in how the focal issue will evolve.

Again, students can use their previous list and/or tailor or augment it to include the most relevant grouping of factors. For this case, those notional groups of factors included the following:

- Kuchma's maneuvering.
- Expected candidates and their bases of support.
- Role of the media.
- Russian influence.
- US/EU/Western influence.
- Business interests.
- Nongovernmental organizations.
- Popular sentiment.

Step 4: Write a brief description of each or use the descriptions previously developed.

Kuchma's maneuvering: Kuchma is taking steps to alter the constitution to deprive the new president of significant powers. Kuchma has been accused in the past of unscrupulous dealings, raising questions about just how far he will go to ensure Yanukovych's victory and how effective he might be in doing so. Would he try to prolong his own rule by provoking a crisis? Would he take ruthless steps to silence the opposition? Or would he attempt to divide the opposition by wooing one or more of its significant members away from Yushchenko's camp?

Expected candidates and their bases of support: How the candidates conduct their campaigns, including their ability to garner support from voters and business leaders, will affect voter turnout and financial support. The degree of corruption and fraud are key unknowns.

Role of the media: The media are largely controlled by the government in Ukraine and present few, if any, opposing political viewpoints. The opposition at their February convention showed a creative use of technology and nontraditional media to broadcast their message. Also, there is an underlying assumption that control of the media will only help the incumbent, when it is possible that the lack of alternative perspectives could encourage an engaged electorate to seek out nontraditional sources of information. A gap that additional research could fill is the extent to which the opposition is tapping other forms of communication and, if it is, what these forms of communications are.

Russian influence: The case narrative highlights strong motivations to discourage a Yushchenko presidency, but the case does not identify specifically Russia's potential means for influencing a transition. Russia's means of influencing the outcome and indications that Moscow is exercising those means are an avenue for further research. If Russia sees Ukraine as its most important foreign policy issue, how far will it go to protect its interests in Ukraine?

US/EU/Western influence: The United States and other Western countries, including international organizations, have provided aid—via foreign NGOs and international institutions such as the Council of Europe, the OSCE, etc.—to fledging civil society organizations in other countries. To what extent are they funding these organizations in Ukraine and to what effect?

Business interests: Ukrainian businesspeople are in a position to influence the election by providing financial support to the candidates and enabling access to the media. Some businesspeople have withdrawn their support for Yanukovych and are backing Yushchenko. Which businesspeople are supporting the main candidates, how strong is their support, and how might their support tip the balance in one direction or the other?

Nongovernmental organizations: NGOs are operating in Ukraine. To what extent can NGOs organize the kinds of activities that took place in Georgia's Rose Revolution? To what extent is Kuchma taking preemptive action to prevent such activities?

Popular sentiment: How does the Ukrainian electorate perceive the candidates and the contest in general? What are their perceptions of Western or Russian involvement? And what will be their level of voter turnout and activism?

Step 5: Generate a matrix with the list of drivers down the left side, as shown in Table 16.3.

Step 6: Generate at least four different scenarios: a best case, a worst case, mainline, and at least one other.

Table 16.3 ▶ Ukraine Simple Scenarios Example

	Best Case "Democratic Transition"	Worst Case "Constitutional Coup"	Mainline "Triumph of the Oligarchs"	Additional "Ukraine's Rose Revolution"
Leonid Kuchma's Maneuvering		+	+	–
Viktor Yanukovych		+	+	–
Viktor Yushchenko	+	–	–	+
Role of the Media	+	+	+	+
Russian Influence		+	+	–
Western Influence	+	–	–	+
Ukrainian Business Interests		+	+	+
Nongovernmental Organizations	+	–	–	+
Popular Sentiment	+			+

Note: "+" = strong or positive influence; "–" = weak or negative influence; no entry = blank or no change.

- Best Case: "Democratic Transition."
- Worst Case: "Constitutional Coup."
- Mainline: "Triumph of the Oligarchs."
- Additional: "Ukraine's Rose Revolution."

Step 7: The columns of the matrix are used to describe the scenarios. Each scenario is assigned a positive or negative value for each driver. The values are strong or positive (+), weak or negative (−), and blank if neutral or no change. An easy way to code the matrix is to assume that the scenario occurred and ask, "Did driver *A* exert a strong, weak, or neutral influence on the outcome?"

Step 8: This is a good time to reconsider both the drivers and the scenarios. Is there a better way to conceptualize and describe the drivers? Have any important forces been omitted? Look across the matrix to see the extent to which each driver discriminates among the scenarios. If a driver has the same value across all scenarios, it is not discriminating and should be deleted or further defined. To stimulate thinking about other possible scenarios, consider the key assumptions that were made when deciding on the most likely scenario. What if some of these assumptions turn out to be invalid? If they are invalid, how might that affect the outcome, and are such alternative outcomes included within the available set of scenarios?

For the purposes of the matrix, it is best to disaggregate the candidates so that Yushchenko's opposition and Yanukovych's government-supported maneuvering are independent drivers. The media have the same value across all scenarios, which might have marked the driver for deletion, but in this case, the media's role can vary widely. As a result, the driver should be retained, and the variation should be described in the story for each scenario. For example, in the story for the best-case scenario, state media coverage is heavily tilted toward Yanukovych, but Yushchenko receives some coverage and significant funding from some oligarchs. In the alternative scenario, on the other hand, Yushchenko is shut out from the mainstream media, but his following grows through public appearances and his Internet presence.

One interesting outcome of this coding exercise is the similar coding for the worst-case and mainline scenarios. Upon further examination, this is because a fundamental assumption for both is that the presidency is "stolen," whether through maneuvering in the legislature or through unfair and fraudulent conduct of the election.

Step 9: For each scenario, write a one-page story to describe what the future looks like and/or how it might come about. The story should illustrate the interplay of the drivers.

Key elements in the one-page stories for the four scenarios we have generated might include these:

Best case ("democratic transition"): Elections are held as scheduled. The campaigns proceed with little discord. State media coverage is heavily tilted toward Yanukovych, but Yushchenko receives some coverage and significant funding from some oligarchs, including Dnipropetrovs'k clan leader Viktor Pinchuk. Russia sends funding to Yanukovych but refrains from blatant interference or endorsement, hoping to leave the door open to pragmatic relations with whoever wins the election. Kuchma fails to win two-thirds majority approval of the Rada for the constitutional reform bill. Pressure from the OSCE, the Council of Europe, the United States, and the European Union deters Kuchma from the most egregious options to cook the election books. Meanwhile, the US bilateral relationship with Russia improves and includes a pledge by both sides to respect the will of the Ukrainian people on both the presidential election and NATO membership.

Worst case ("constitutional coup"): The Rada approves the constitutional reform bill by a vote of 300–0, with "Our Ukraine" and other opposition groups boycotting the vote. True to his word, Yushchenko, along with Tymoshenko, leads a massive campaign of protests and civil disobedience. Aside from several thousand demonstrators in Kyiv, however, the Ukrainian people are unmoved, and Kuchma seizes the opportunity to declare a state of emergency. Kuchma strikes a deal with Russia to join the Common Economic Space and gets a long-term gas deal on favorable price terms for Ukraine. In response to Western criticism, Kuchma pulls Ukrainian troops from Iraq, and Putin offers direct support of Kuchma's actions by crediting Kuchma's "strong leadership" in averting a full-blown crisis.

Mainline ("triumph of the oligarchs"): Kuchma's constitutional reform bill fails by a narrow margin. Donetsk clan head Renat Akhmetov strikes a deal with Dnipropetrovs'k clan head Viktor Pinchuk, aligning all of Ukraine's business clans behind Yanukovych. Kuchma chief of staff Medvedchuk travels to Moscow in April to get a briefing from Russia's intelligence chiefs on the lessons learned from the Rose Revolution in Georgia, and the regime cracks down on foreign NGOs and arrests leaders of a nascent youth

organization in May. In August, key Yushchenko ally Yulia Tymoshenko dies in a car bombing, and Kuchma's past involvement in the killing of opposition journalist Gongadze prompts speculation that his government arranged the assassination. With US and EU support, the OSCE withdraws its election-monitoring team, declaring that the new circumstances preclude a free and fair election. Yushchenko manages to qualify for a runoff election in the first round of voting on 31 October, but he loses the runoff vote to Yanukovych. Ukrainian NGOs claim the vote involved massive fraud, but the regime precludes alternative vote count efforts, and opposition calls for protest spark little action from the public.

Additional scenario ("Ukraine's Rose Revolution"): Kuchma's constitutional reform bill falls short of winning a two-thirds majority in the Rada. Ukraine's oligarchs align in support of the Yanukovych campaign, and Russia intervenes heavily in support of Yanukovych, fueling a nationalist backlash that benefits the Yushchenko candidacy. It also reinforces the determination of international organizations and Western-financed NGO groups to organize alternative vote counts and strict election monitoring. Activists from Georgia's Rose Revolution train their Ukrainian counterparts in civic organization and popular mobilization. Yushchenko is shut out from the mainstream media, but his following grows through public appearances and his Internet presence. Much as in Georgia's Rose Revolution, the regime claims its candidate won the election, but the public protests against the perception of massive fraud and the government cannot rely on security forces to stop the demonstrators, who peacefully take over state television and key ministries and declare Yushchenko president. Sensing the inevitable, Yanukovych concedes the election to Yushchenko, and Kuchma and his key associates flee to Russia.

Step 10: For each scenario, describe the implications for the decision maker. The implications should be focused on variables that the United States could influence to shape the outcome.

Following are some examples:

- **Best case ("democratic transition"):** US diplomatic outreach to Russia and a bilateral agreement to respect the Ukrainian democratic process are key means of holding Russian influence in abeyance.
- **Worst case ("constitutional coup"):** The key variable in this scenario is the vote in the Rada, over which the United States exerts little influence.
- **Mainline ("triumph of the oligarchs"):** The withdrawal of the election-monitoring team removes the key means through which the United States can encourage free and fair elections.
- **Additional ("Ukraine's Rose Revolution"):** Engagement via election monitoring and support to civil society organizations helps ensure a democratic process can be followed, if the sides allow it to be. These organizations can be encouraged to use nontraditional media to get their message out.

Step 11: Generate a list of indicators for each scenario that would help you discover that events are starting to play out in the way envisioned by the scenario.

Some general indicators might include the following, but instructors should encourage analysts to define the indicators with as much specificity as possible. For a more robust indicators process, employ a full Indicators and Indicators Validator™ process.[1]

- **Best case ("democratic transition"):** State institutions uphold the letter and intent of law. Instances of harassment attributed to the government are rare. Few complaints are filed with the Central Election Commission. Opposition media flourishes and gains a stronger representation among sources of information. Russia takes a hands-off approach.
- **Worst case ("constitutional coup"):** The constitutional reform bill passes. Instances of violence during the campaign occur against both candidates. Government institutions take measures to strengthen presidential powers.
- **Mainline ("triumph of the oligarchs"):** The oligarchs resist the urge to split their forces and resources and instead remain united in support of Yanukovych. State and partisan lines are blurred. Instances of violence during the campaign intimidate the opposition and reduce turnout for or frequency of rallies.
- **Additional ("Ukraine's Rose Revolution"):** Opposition media do not cower in response to intimidation. New media sources pop up as others are shut down or their operations are constrained by government activities. New media sources are used as an organizing force by opposition groups. The oligarchs split their support for the main candidates. The Russians play a vocal, partisan role in favor of Yanukovych; there are signs of a popular backlash in support of Yushchenko. The opposition redoubles its

efforts in the face of intimidation tactics resulting in more rallies, more media coverage, and higher voter turnout.

Step 12: Monitor the list of indicators on a regular basis.

Analytic Value Added: What judgments should analysts highlight in response to US policy makers' questions about what will influence the outcome of the Ukrainian election? It is often helpful to advise students before they embark on this portion of the exercise that forecasting is one of the hardest tasks an analyst faces. The Simple Scenarios technique is not a means that will produce a "result" that can then be parroted to policy makers. Rather, the technique is designed as a means to identify and actively consider how each outcome could come about. This process can help the analyst know—and warn policy makers—if one future or another is emerging. The goal is to help policy makers understand the dynamics at play and the most plausible outcomes that can be produced by various permutations of the dynamics.

Analysts should therefore identify not only the implications identified in the exercise but also the key indicators that would suggest that an outcome is occurring. For example, the level and nature of Russian involvement—an external factor—figure as a key driver in several scenarios. Students should be able to define the hallmarks of Russian behavior that would contribute to the relevant scenarios. In the best-case scenario, Russia would take a relatively hands-off approach, while in the worst-case scenario, the Russians would most likely aid and abet Kuchma's grip on power.

Another way to test the students' understanding of the analytic value added is to have them develop a graphical representation of the key findings of the previous three exercises. This exercise encourages analysts to distill the key judgments, drivers, and assumptions about the range of possible outcomes rather than create a tome that simply summarizes the results.

Yet another means of testing students' understanding is to ask them how confident they are that a particular outcome will occur. Then ask what would need to occur to increase or decrease their confidence. This questioning method often helps students identify indicators, gaps, and assumptions that they have not yet considered. Next, ask them how they could track the indicators, close the gaps, and check the assumptions that they have identified. This process can become the basis for an information collection strategy that will guide further research.

CONCLUSION

Ukraine's presidential transition wound up producing what became known popularly as the "Orange Revolution," but in retrospect it is apparent that this outcome was far from preordained; several other alternative scenarios came close to being realized (see Figure 16.5 for a chronology of this period). Constitutional reform, for example, proved to be a near miss. On 8 April 2004, Ukraine's Rada fell just six votes short of the two-thirds majority needed to pass Kuchma's constitutional reform bill.[2] Opposition blocs boycotted the vote, and the government failed to garner enough support from independent deputies to carry the day. The Rada chair declared the bill dead until sometime after the presidential elections, and the leaders of pro-government parties in the legislature voted to unite behind Yanukovych's candidacy.[3]

The campaign turned out to be a bare-knuckled contest. The government's intended tactics became clear in the mayoral election in Mukachevo held in April, when the regime employed "gross falsifications" and "pure thuggery" at the polling stations to defeat a popular Yushchenko ally, alarming opposition groups.[4] As the presidential campaign progressed over the summer into the fall, Kuchma's operators pulled out all the stops to bolster Yanukovych, but many of their tactics proved counterproductive. The government regularly issued so-called *temnyky*—informal guidance on coverage—to media organizations. State-controlled television coverage amounted to little more than crude propaganda, and the refusal to broadcast Yushchenko only encouraged larger attendance at his campaign events by voters curious to learn about him.[5] Yushchenko's campaign also faced near-constant harassment. At one point, a truck attempted to force his motorcade from the road, and in September he was taken ill with a mysterious malady that nearly took his life. Austrian doctors diagnosed the illness as dioxin poisoning; Yushchenko accused the Kuchma regime of involvement, but the perpetrators were never identified. The poisoning left Yushchenko's once handsome face badly scarred, but it also cemented his image as a courageous opponent of the regime's brutality and redoubled his determination to win the presidency.[6]

Like the Kuchma regime, Russia intervened massively in support of the Yanukovych campaign, but if anything its efforts backfired. To all appearances, Russian President Putin made the Ukrainian election a personal mission, meeting with Kuchma on an almost monthly basis during

the campaign, coming out publicly in favor of Yanukovych in July, and even campaigning for Yanukovych in Ukraine on the eve of the election.[7] Dozens of Russian political consultants descended upon Ukraine, appearing frequently on Ukrainian- and Russian-language television shows praising Yanukovych and criticizing Yushchenko.[8] Hundreds of millions of dollars in Russian money poured into Yanukovych campaign coffers.[9] The Kremlin's campaign came across as a transparent attempt to impose its will on Ukraine and may actually have hurt Yanukovych.[10]

Arrayed against the Kuchma regime, Russia, and Yanukovych were Ukraine's opposition groups and a range of NGOs. For several years, the United States, Europe, and private donors had been funding Ukrainian NGOs involved in voter education, judicial reform, and election monitoring, and these groups in turn had developed an extensive network of local activists and officials trained in election laws and community organization.[11,12] In parallel, several independent Internet media sites were established, including the cyber-newspaper *Ukrainska Pravda*, which became a key source of news on the Yushchenko campaign, and the website Maidan, which served as a "virtual civic organization in cyberspace" for regime opponents.[13] In late March 2004, a Ukrainian student organization named *Pora* ("It's Time") emerged, modeled on groups that had helped to topple presidents in Serbia and Georgia; it provided both formal and informal support for the Yushchenko campaign, despite harassment by the regime that *Pora* activists sometimes captured on cell-phone cameras.[14] The United States adopted a neutral stance toward the candidates but pressed the Kuchma government to ensure a free and fair electoral process.[15] In May 2004, then Deputy Assistant Secretary of State Steven Pifer told the House International Relations Committee's Subcommittee on Europe that

> the US Government does not back any particular candidate in the election; our interest is in a free and fair electoral process that lets the Ukrainian people democratically choose their next president. We would be prepared to work closely and eagerly with whomever emerges as president as the result of such a process.[16]

He added that "the single most important issue now on our bilateral agenda is the conduct of the Ukrainian presidential campaign and election" and "the upcoming presidential election . . . will affect Ukraine's strategic course for the next decade."[17] Monitors from the Organization for Security and Cooperation in Europe (OSCE) worked toward this end on the ground, keeping a watchful eye on the conduct of the campaign and the preparations for voting.[18]

The voting on 31 October divided the country. It produced a virtual tie between the two leading candidates, with Yushchenko officially garnering 39.90 percent of the vote compared to 39.26 percent for Yanukovych. Yanukovych won 71 percent of votes in the east and south, and Yushchenko took 78 percent of the western and central regions. OSCE monitors reported numerous irregularities, and fed-up journalists at state-run television stations balked at obeying the regime's *temnyky,* signaling important fractures in the Kuchma government's power base.[19,20] The precipitous drop in votes for Communist candidate Symonenko compared to both his own performance in 1999 and his party's support in the 2002 Rada election suggested that some of his votes had been fraudulently reallocated to Yanukovych, and an enraged Symonenko urged his supporters to vote against both candidates in the run-off election that was to be held on 21 November, as required by Ukraine's election laws.[21]

The run-off was marred by massive falsification.[22] The Central Electoral Commission declared Yanukovych the winner with 49.5 percent of the vote versus 46.6 percent for Yushchenko. Opposition groups immediately rejected the results, citing independent exit polls that indicated Yushchenko had won 53 percent of the vote. Critics highlighted the implausibility of turnout numbers in Ukraine's east regions, particularly in Yanukovych's home region of Donetsk, where voting supposedly increased by more than 18 percent over the first round to a whopping 96 percent of eligible voters, nearly all of whom allegedly sided with Yanukovych.[23] Yushchenko immediately called for protests against the fraud, and some 5,000 of his supporters set up tents on Kyiv's main square shortly after the polls had closed on the evening of 21 November.[24]

It quickly became apparent that the regime faced a daunting challenge. By the morning of 22 November, 200,000 protestors had come to Maidan square, rallied by Yushchenko's appeals to the country broadcast through cell phones and the Internet, as well as by mainstream media journalists who had joined the opposition.[25] Clad in orange, the protestors grew in number by the day, and within a week more than one million "orange revolutionaries" had gathered in central Kyiv, blocking government ministry buildings and insisting that Ukraine's Supreme Court invalidate the vote. Organizers constructed facilities to house and feed the protestors and established a system of

Figure 16.5 ▶ Chronology of Selected Events, March 2004–January 2005

Date	Events
2004	
18 March	Parliament votes to hold elections on 31 October 2004.
Late March	*Pora* ("It's Time") youth movement emerges publicly.
1 April	Viktor Pinchuk and George Soros announce plans to combine philanthropic efforts by forming legal aid society.[i]
16 April	Viktor Medvedchuk meets Russian President Vladimir Putin at the Kremlin. Putin supports will of people but says he prefers continuity in the bilateral relationship.[ii]
23 April	Putin visits Ukraine, meets with Leonid Kuchma.[iii]
23–24 May	Putin visits Ukraine for meetings on Single Economic Space.
3 July	Presidential election campaign officially begins.
26 July	Kuchma, Viktor Yanukovych, and Putin meet in Yalta.
5 September	Viktor Yushchenko falls ill after dinner with the head of the Ukrainian Intelligence Service.
24 September	Yanukovych struck in chest with an egg, hospitalized for several hours, and released.
15–16 October	*Pora* youth organization offices raided by government special police.[iv] Kuchma meets with Putin in Sochi.
20 October	Pro-opposition Channel 5 assets frozen by government; journalists go on hunger strike.[v]
23 October	Yushchenko holds mass rally outside Central Election Commission (CEC).
24 October	A group of 100 journalists marches in support of Channel 5. Separately, a bottle of combustible liquid is hurled into Yushchenko's chief of staff's car in Kyiv. The Ukrainian CEC votes unanimously to establish forty-one exceptional voting sites in the Russian Federation.[vi]
25 October	*Pora* announces a wave of student protests and actions for 25–30 October in response to alleged government intimidation.
26 October	Putin begins multiday visit to Ukraine.
28 October	Supreme Court overturns CEC decision on exceptional voting sites in the Russian Federation.[vii]
31 October	First round of presidential election held. Voting in the presidential election gives Yushchenko a small lead against Yanukovych and triggers a second-round vote. OSCE says the vote fails to meet a considerable number of Ukraine's OSCE commitments.
21 November	Second round runoff presidential election held. It triggers a flurry of fraud accusations.
22 November	The Central Electoral Commission declares Yanukovych the winner, and Yushchenko supporters take to the streets.
25 November	Supreme Court suspends publication of the voting results by the CEC following a complaint by Yushchenko.
26 November	Yanukovych and Yushchenko agree to seek a peaceful solution.
1 December	Yushchenko lifts a blockade on government buildings and encourages his supporters to remain on the streets.
3 December	Supreme Court annuls results of second round, paving the way for new elections.
11 December	Doctors in Vienna confirm that dioxin is the cause of Yushchnko's poisoning.
26 December	Repeat second round of presidential elections held. OSCE notes improvements.
2005	
11 January	CEC announces the election results and names Yushchenko the winner.
20 January	Yanukovych concedes.
23 January	Yushchenko is sworn in as president.

i. "George Soros, "Viktor Pinchuk to Create Legal Aid Foundation in Ukraine," US-Ukraine Business Council. April 1, 2004, http://www.usubc.org/AUR/aur4–052.php.

ii. "Russia Watches Ukraine Election," *Ukraine Weekly,* May 30, 2004, http://www.ukrweekly.com/.

iii. "Putin: Broadcasting Not an Issue," *Ukraine Weekly,* May 9, 2004, http://www.ukrweekly.com/.

iv. Andrew Wilson, *Ukraine's Orange Revolution* (New Haven, CT: Yale University Press, 2006), 76.

v. "Ukraine TV Station on Hunger Strike Ahead of Poll," Reuters, October 27, 2004.

vi. Organization for Security and Cooperation in Europe (OSCE), "Ukraine Presidential Election OSCE/ODIHR Election Observation Mission Final Report," May 11, 2005.

vii. Ibid.

self-policing and security, providing no pretexts for a government crackdown.[26]

The Kuchma regime scrambled to regain control of events, but it soon became clear that the regime's options for dealing with the protests were sharply constrained. Dnipropetrovs'k clan leader Viktor Pinchuk defected from the ranks of Yanukovych supporters, dealing a critical blow to the regime's hopes.

Within Ukraine, one force after the other abandoned the authorities. One early group of official defectors was Ukrainian diplomats. The armed forces split. Two former SBU (Ukraine's intelligence service) generals spoke in favor of the opposition in Maidan square on 25 November, and the SBU leadership seemed to follow. The same day, the commander of Ukraine's Western Military Command declared that his troops would not be used against the nation, indicating that the military was regionally divided, as were the civilian police. The regime could deploy only select special forces of the Ministry of Interior for a crackdown.[27]

Sensing the inevitable, Kuchma entered negotiations with key parties to reach a settlement. The presidents of Poland and Lithuania joined as mediators, and Yanukovych invited Russia's Duma Speaker as well. To facilitate a deal, Yushchenko agreed to a reduction of presidential power, transferring some key authorities to the Rada.[28] Both sides agreed to let Ukraine's Supreme Court—more independent than the Kuchma-controlled Constitutional Court—rule on the conduct of the elections. On 3 December, the Supreme Court ruled that the government had conducted massive fraud and invalidated the election results, and it called for a repeat runoff election on 26 December.[29] Yushchenko won that repeat election handily, in a vote characterized by OSCE monitors as largely free and fair.

President Yushchenko took office in January 2005. The Orange Revolution was over. The difficult task of governing a divided country, with a newly empowered legislature, remained.

KEY TAKEAWAYS

- External or indirect forces are easy to overlook, but they can have a significant effect on the outcome. Using techniques like Outside-In Thinking can illuminate these forces early in the analytic process and provide an opportunity to track their development.
- Analytic forecasting is one of the hardest tasks that an analyst can face. Use Simple Scenarios to overcome the temptation to narrow the focus of analysis prematurely on a single outcome.

NOTES

1. Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis,* 2nd ed. (Washington, DC: CQ Press, 2015, 149).
2. Roman Woronowycz, "Verkhovna Rada Fails, by 6 Votes, to Pass Constitutional Amendments," *Ukraine Weekly*, April 11, 2004, http://www.scribd.com/doc/12815581/The-Ukrainian-Weekly-200415.
3. Roman Woronowycz, "Majority Coalition Taps Yanukovych as Presidential Candidate," *Ukrainian Weekly,* April 18, 2004, http://www.scribd.com/doc/12815982/The-Ukrainian-Weekly-200416.
4. Nadia Diuk, "The Triumph of Civil Society," in *Revolution in Orange: The Origins of Ukraine's Democratic Breakthrough*, Anders Äslund and Michael McFaul, eds. (Washington, DC: Carnegie Endowment for International Peace, 2006), 78.
5. Anders, Äslund, *How Ukraine Became a Market Economy and Democracy* (Washington, DC: Peterson Institute for International Economics, 2009), 180–84.
6. Adrian Karatnycky, "Ukraine's Orange Revolution," *Foreign Affairs*, March–April 2005, http://www.foreignaffairs.com/articles/60620/adrian-karatnycky/ukraines-orange-revolution.
7. Andrew Wilson, *Ukraine's Orange Revolution* (New Haven, CT: Yale University Press, 2005), 86–95.
8. Äslund, *How Ukraine Became a Market Economy and Democracy*, 183.
9. Ibid., 182–83.
10. Nikolai Petrov and Andrei Ryabov, "Russia's Role in the Orange Revolution," in *Revolution in Orange: The Origins of Ukraine's Democratic Breakthrough,* Anders Äslund and Michael McFaul, eds. (Washington, DC: Carnegie Endowment for International Peace, 2006), 145.
11. Jeffrey Clark (with Jason Stout), *Elections, Revolution, and Democracy in Ukraine: Reflections on a Country's Turn to Democracy, Free Elections, and the Modern World* (Arlington, VA: Development Associates, 2005).
12. Diuk, "The Triumph of Civil Society," 75.
13. Ibid., 73.
14. Wilson, *Ukraine's Orange Revolution*, 75.
15. Roman Woronowycz, "Armitage to Kuchma: Free and Fair Elections Will Be Benchmark of US-Ukraine Relations," *Ukraine Weekly*, April 4, 2004.
16. Steven Pifer, "Ukraine's Future and US Interests," testimony before the House International Relations Committee, Subcommittee on Europe, May 12, 2004, http://2001–2009.state.gov/p/eur/rls/rm/32416.htm.
17. Ibid.

18. Organization for Security and Co-operation in Europe (OSCE) Office of Democratic Institutions and Human Rights (ODIHR), *Ukraine Presidential Election: OSCE/ODIHR Election Observation Mission Final Report* (Warsaw, Poland: OSCE ODIHR, 2005), http://www.osce.org/odihr/elections/ukraine/14674.

19. Ibid.

20. Äslund, *How Ukraine Became a Market Economy and Democracy*, 190.

21. Ibid.

22. OSCE ODIHR, *Ukraine Presidential Election*.

23. Äslund, *How Ukraine Became a Market Economy and Democracy*, 191.

24. Diuk, "The Triumph of Civil Society," 80.

25. Äslund, *How Ukraine Became a Market Economy and Democracy*, 192.

26. Diuk, "The Triumph of Civil Society," 80.

27. Äslund, *How Ukraine Became a Market Economy and Democracy*, 194.

28. Timothy Garton Ash and Timothy Snyder, "The Orange Revolution," *New York Review of Books*, April 28, 2005, http://www.nybooks.com/articles/archives/2005/apr/28/the-orange-revolution.

29. Äslund, *How Ukraine Became a Market Economy and Democracy*, 195.

Table 17.1 ▶ Case Snapshot: Violence Erupts in Belgrade		
Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Force Field Analysis	p. 304	Decision Support
Decision Matrix	p. 297	Decision Support
Pros-Cons-Faults-and-Fixes	p. 300	Decision Support

17 Violence Erupts in Belgrade
Cases in Intelligence Analysis: Structured Analytic Techniques in Action
Instructor Materials

This case puts students in the shoes of US diplomats in Belgrade at the time of Kosovo's declaration of independence in 2008. Although these Instructor Materials provide a "school solution" that describes the actual outcome at the time, the key objective of the case is not to re-create or reexamine specific US decisions but to help students learn to conduct a logical and thorough decision-support process.

Many of the most important decisions are made quickly and under tight time constraints. This does not mean that decision makers or those supporting them should sacrifice good thinking, because a logical and thorough thought process is a fundamental element of devising the best course of action, even when the circumstances in which the decision is being made are less than ideal. The following techniques and exercises provide a template for a solid decision process by using Force Field Analysis, a Decision Matrix, and Pros-Cons-Faults-and-Fixes to identify and assess the problem, consider a range of options, and troubleshoot the decision.

TECHNIQUE 1: FORCE FIELD ANALYSIS

A Force Field Analysis is a decision tool that can be used to identify and assess the key forces and factors that are driving or constraining a particular outcome. By exhaustively listing and weighting all the forces for and against an issue or outcome, analysts can more thoroughly define the forces at hand. In addition, the technique helps analysts assess the relative importance of each of the forces affecting the issue. A clearer understanding of these forces can in turn be used to fashion a course of action that augments particular forces to achieve a desired outcome or diminishes forces to reduce the chances of an undesirable outcome.

Task 1.

Conduct a Force Field Analysis of the factors for and against additional violence directed at US interests in Belgrade.

Step 1: Define the problem, goal, or change clearly and concisely.

In this case, the initial problem at hand by Tuesday, 19 February, is to determine whether the violence against US and other Western interests in Belgrade will increase and, if so, what the US embassy should do to maintain building security, protect its personnel, and advance its policy objectives. A Force Field Analysis should therefore focus on the forces driving and constraining additional violence against the US embassy.

Step 2: Use a form of brainstorming to identify the main factors that will influence the issue.

Using Structured Brainstorming,[1] students should generate an exhaustive list of forces, factors, and issues that will affect the chances of more violence. Encourage students to jumpstart their brainstorming by using STEEP +2 (Social, Technological, Economic, Environmental, Political plus Military and Psychological). The process should prompt a discussion of information gaps and assumptions that require further research or require refinement of the forces and/or groupings.

Step 3: Make one list showing the strongest forces for and against additional violence.

For this case, some of the key forces for additional violence include the following:

- Formal US and European recognition of Kosovo's unilateral declaration of independence.
- Serbian officials' strong anti-Western rhetoric.

- Reports of a secret action plan that includes a provision for Serbs to reject Kosovo's declaration of independence.
- The failure of Serbian riot police to avert damage to Western assets on Sunday and Monday.
- The opportunity for splinter groups to use the government-sponsored peaceful demonstration planned for Thursday evening to perpetrate violence.

Forces against violence include these:

- Antiriot police actively attempted to repel attackers on Sunday and Monday.
- Serbian officials have urged calm and called for a peaceful demonstration on Thursday.
- Serbia's EU aspirations should constrain any government impulse to endorse or facilitate violence or military action.
- The vast majority of the demonstrators on Sunday were peaceful.

Step 4: Array the lists in a table such as Table 17.5.

Step 5: Assign a value to each factor to indicate its strength. Assign the weakest intensity scores a value of 1 and the strongest a value of 5. The same intensity score can be assigned to more than one factor if the factors are considered equal in strength.

The intensity-scoring process is an opportunity to discuss the underpinning assumptions and gaps in the arguments for and against the outcome. In this case, a discussion of the performance of Serbian antiriot police on Sunday and Monday reveals that while they were able to repel the rioters, the police were not able to prevent the rioters from causing damage. As a result, police performance is reflected on both sides of the ledger, and future performance is therefore a key uncertainty. In this case, a fairly high intensity score of 4 is given to the police as a constraining force, but this assumes ability and willingness to repel future rioters. Also, although Serbian officials have urged calm and called for a peaceful demonstration on Thursday, a factor given a high constraining intensity score, Serbian media are focusing on anti-US and anti-Western messages. Given the strong anti-US rhetoric used by some Serbian officials and the Serbian police's spotty performance during the Sunday attack, the assumption that Serbians have both the willingness and ability to repel future attacks is not a strong one and should carry caveats to reflect this uncertainty.

Other drivers that receive high intensity scores include formal US recognition of Kosovo, which received media attention worldwide, and ongoing sharp anti-US rhetoric. Both stoked already high emotions.

Table 17.5 ▶ Violence in Belgrade Force Field Analysis Example

Issue: Forces For and Against Additional Violence Against US Interests in Serbia			
Score	Forces Driving More Violence Aimed at the US Embassy	Forces Constraining More Violence Aimed at the US Embassy	Score
5	The United States has officially recognized Kosovo's unilateral declaration of independence.	The antiriot police actively attempted to repel attackers on Sunday night and on Monday.	4
5	Serbian officials are using sharp anti-US rhetoric and denouncing the independence move.	Serbian officials have urged calm and called for a peaceful demonstration.	4
3	There are reports of a secret action plan with retaliatory steps calling for Serbs to reject Kosovo independence.	Serbia's EU aspirations should limit the threat of state-facilitated violence or military action.	4
3	Peaceful Serbian government-backed demonstration planned for late in the day Thursday is an opportunity for splinter groups to become violent.	The vast majority of the demonstrators on Sunday were peaceful.	3
4	Antiriot police were unable to avert damage to Western assets on Sunday and may fail again.		
Total: 20			Total: 15

Step 6: Calculate a total score for each list to determine whether the arguments for or against are dominant.

Step 7: Examine the two lists to determine whether any of the factors balance out each other.

Students may be tempted to argue that the contrasting public comments by Serbian officials urging calm and stoking anti-US sentiment counterbalance each other. This example illustrates the importance of careful consideration of the intensity variable. Assigning an intensity score to Serbian officials' comments is problematic absent an understanding of their intended audiences and the likely impact. The most prominent advocate of restraint in this episode is President Tadic, but his counsel against violence was made about the time of his travel to New York to meet with the UN Security Council and was arguably aimed more at international than Serbian audiences. Koštunica's sharper anti-US rhetoric was broadcast on national television and appeared aimed at Serbs, who cared at least as much about perceived injustice at the hands of Washington and Europe as they did about Kosovo's status. The splinter groups most prone to violence are more likely to be moved to action by the anti-US rhetoric than they are to be constrained by calls for calm.

Step 8: Analyze the lists to determine how changes in factors might affect the overall outcome.

A key factor is the opportunity that the Thursday demonstration presents for further violence. If the Thursday demonstration is cancelled, postponed, or poorly attended because of inclement weather, momentum toward violence may be lost, and the importance of the riot police as a driving force could diminish. This would cause the factors constraining violence to at least counterbalance, if not outweigh, the forces driving violence.

Task 2.

Answer these questions:

- Which forces are the strongest?
- Do any assumptions underpin your intensity scores?
- Are there uncertainties that could affect your analysis, and if so, what are they?

The strongest forces include US recognition, which has already occurred, and the Serbian leadership's reaction. A key assumption and corollary are that the Thursday demonstration provides an opportunity for a repeat of Sunday night's violence and that the riot police will again be challenged to repel the attackers. Key uncertainties include the potential performance of the riot police and whether Serbian authorities have both the ability and willingness to avert further violence.

Analytic Value Added: Is additional violence against US interests in Belgrade likely? Serbian authorities' plans for a large-scale demonstration, coupled with sustained anti-US rhetoric, could serve as catalysts for further violence aimed at US interests in Belgrade. A key uncertainty, however, is the performance of the Serbian police, assuming that the mass rally sparks an even larger number of rioters than on Sunday.

TECHNIQUE 2: DECISION MATRIX

A Decision Matrix helps identify a course of action that maximizes specific goals or criteria. This technique breaks down a decision into its component parts by listing all the options or possible choices and the criteria for judging the options. It uses weights to help analysts determine the extent to which each option satisfies each of the criteria relative to the other options. Although the matrix results in a quantitative score for each option, the numbers do not make the decision. Instead, they should be used to guide a decision maker's understanding of the trade-offs among the various and often competing goals, or criteria, and how an option might be modified to best meet those goals.

Task 3.

Use a Decision Matrix to assess how the US diplomats in Belgrade should respond to the threat of additional violence.

Step 1: Identify the decision or question to be considered.

What is the best way for the United States to protect US security and policy objectives vis-à-vis Serbia in light of the assessment that additional violence is possible?

Step 2: List the selection criteria and options. The number of criteria and options can vary from case to case.

Criteria:

1. Protect US embassy (e.g., physical buildings, information).
2. Protect US persons (e.g., staff, dependents, foreign service nationals).

3. Pursue US policy position vis-à-vis Kosovo and Serbia (i.e., stand by recognition of Kosovo).
4. Minimize economic costs to US embassy.

Options:

1. Withdraw ambassador (tit-for-tat withdrawal).
2. Close the embassy to the public but keep operating otherwise.
3. Administratively close the embassy on Thursday; that is, close it to the public and send home nonessential staff.
4. Close the embassy and evacuate dependents.

Step 3: Consolidate items within each list to eliminate overlap among the items.

Step 4: Fill in a matrix like the example in Table 17.6 with the criteria and options you have generated.

Step 5: Assign a weight to each criterion based on the relative importance of each. An easy way to do this is to divide 100 percentage points among the criteria.

Working in whole numbers, rather than percentages, considerably simplifies the math. We have assigned a weight of 35 to both personnel and policy to reflect the emphasis the United States places on both personnel protection and its long-standing policy on Kosovo. Physical security received a score of 20 because, while important, providing the first line of protection will still fall to the local authorities. Economic cost received a score of 10 because while it is a factor, its importance is relatively less than that of the other factors.

Step 6: Work across the matrix one row at a time to evaluate the relative ability of each of the options to satisfy each criterion. To do so, assign 10 points to each row and divide these points according to an assessment of the ability of each option to satisfy the selection criteria.

For example, neither withdrawal of the ambassador nor closing to the public directly protects US personnel if an attack occurs and the majority of personnel are still in the embassy. Administrative closure and total evacuation, however, both have a chance of satisfying this criterion by removing personnel from the premises.

Step 7: Assess the strength of each option against each criterion by multiplying the criterion weight by the assigned strength of the option from Step 6. For example, criterion 1 weight × option 1 points = score. For ease of calculation, simply use the whole number weight rather than a percentage.

Step 8: Determine the total score for each option and enter the sum in the "total" cell at the bottom of the column. The option with the highest total score is the quantitative selection.

Table 17.6 ▶ Violence in Belgrade Decision Matrix Example

		Withdraw Ambassador		Close to Public		Administrative Closure		Close and Evacuate	
Selection Criteria	% Weight (W)	Value (V)	Weighted Value (W x V)	Value (V)	Weighted Value (W x V)	Value (V)	Weighted Value (W x V)	Value (V)	Weighted Value (W x V)
Protect US embassy (physical buildings, information).	20	0	0	4	80	4	80	2	40
Protect US persons (staff, dependents, foreign service nationals).	35	0	0	0	0	5	175	5	175
Pursue US policy position vis-à-vis Kosovo and Serbia.	35	2	70	3.5	122.5	3.5	122.5	1	35
Minimize economic costs to US embassy.	10	5	50	4	40	1	10	0	0
Totals	(100%)		120		242.5		387.5		250

In this example, the administrative closure option is the quantitative selection.

Step 9: Use a qualitative sanity check to help identify key issues, variables, or other observations that could further aid the decision-making process.

Using the same example as above, the analysts' assessment of the scope of potential violence is a key variable that could mean the difference between administrative closure and total evacuation. In the weights given, an underlying assumption is that violence would only be projected at the embassy building itself. If, however, the violence spreads and puts the populace at risk, an administrative closure would not sufficiently protect US persons. As a result, this implicit assumption is a key variable that should be considered.

Analytic Value Added: **Based on your findings, which option best protects US political and security interests in Belgrade, and why?** An administrative closure is most likely the best means to protect US political and security interests because it goes the farthest toward meeting the combined criteria of protecting physical security, protecting personnel, and supporting the US policy position. While it is not the best option to minimize costs, it is not as costly as a total closure and evacuation.

TECHNIQUE 3: PROS-CONS-FAULTS-AND-FIXES

Pros-Cons-Faults-and-Fixes (PCFF) is a simple strategy for evaluating many types of decisions, including policy options. In this case, US officials are presented with an immediate need to respond to violence directed against US interests in the Serbian capital. PCFF is particularly suited to situations in which decision makers must act quickly, because the technique helps to explicate and troubleshoot a decision in a quick and organized manner such that the decision can be shared and discussed by all decision-making participants.

Task 4.

Use PCFF to evaluate the option you chose in Task 3 (see the template for this in Table 17.4). If you have not completed Task 3, use PCFF to evaluate a proposal for how the United States should protect its political and security interests in Belgrade over the week following the February attack on the US Embassy building.

For the purposes of illustrating this technique, we will show how PCFF can be used to troubleshoot the decision to administratively close the Chancery in advance of the Thursday rally.

Step 1: Clearly define the proposed action or choice.

An administrative closure includes the closure of the embassy to the public and all nonessential staff. A skeleton staff remains on-site, including a full US Marine guard detail.

Step 2: List all the Pros in favor of the decision. Think broadly and creatively and list as many benefits, advantages, or other positives as possible. Merge any overlapping Pros.

- This option maintains US diplomatic presence and policy while providing implicit support for Tadic's efforts to chart a pragmatic course that preserves Serbia's EU aspirations. It diplomatically gives the Serbian government the benefit of the doubt that it is both willing and able to protect the embassy per Vienna Convention obligations, and it avoids fueling arguments by Koštunica that the United States is unwilling to work pragmatically with Belgrade.
- It protects the physical structure of the embassy buildings and helps ensure personnel security. It does this by removing nonessential personnel from the premises and allowing the Marines to "batten down the hatches," rather than having the usual stream of employees and visitors in and out of the Chancery.
- While this option is not without cost, it is a relatively economical solution given that the embassy can quickly reopen to staff and visitors once the rally is over and tensions have subsided.

Step 3: List all the Cons or arguments against what is proposed. Review and consolidate the Cons. If two Cons are similar or overlapping, merge them to eliminate redundancy.

- This option assumes that the Serbs will adopt a proactive policy to protect the embassy.
- The embassy lacks a buffer between the building and the sidewalk/street, which makes it particularly difficult for the Marine guards stationed inside to defend the building. The embassy's site also makes it difficult for Serbian police to establish a perimeter or cordon outside.

- If the closure is prolonged, it will reduce productivity, increase costs, and still put the core team and Marines at risk. An extended closure could also project an image of weakness on the part of the United States.

Step 4: Determine Fixes to neutralize as many Cons as possible. To do so, propose a modification of the Con that would significantly lower its risk of being a problem, identify a preventive measure that would significantly reduce the chances of the Con being a problem, conduct contingency planning that includes a change of course if certain indicators are observed, or identify a need for further research or to collect information to confirm or refute the assumption that the Con is a problem.

- Private diplomacy: Reach out diplomatically in private to the Serbians, thank them for the assistance on Sunday, and request a discussion of strategy in advance of Thursday's rally. Couple this outreach with public statements of tempered appreciation for Serb police assistance on Sunday and the ongoing dialogue with the Serb government.
- Public diplomacy: Publicize the Serbian government's responsiveness to Sunday's attacks and the ongoing dialogue between the US and Serbian governments as a deterrent to would-be vandals and a message to Serbia that the United States expects proactive Serbian policing.
- Better safe than sorry: Find a middle approach that protects US persons, policy, and information in the embassy structure while minimizing economic impact. Develop a plan in concert with the US Marines and other possible stakeholders to protect any sensitive information as well as an evacuation plan.

Step 5: Fault the Pros. Identify a reason why the Pro would not work or the benefit would not be received, pinpoint an undesirable side effect that might accompany the benefit, or note a need for further research to confirm or refute the assumption that the Pro will work or be beneficial.

- The Serbians may not have the ability to manage an even larger rally than Sunday's, which could put US interests at risk. Given reports of a "secret plan" and the difficulty that Serb police had dispelling attackers on Sunday, it may not be safe to assume that the Serbian government can manage the situation should another round of riots break out.
- Preemptive closure may provide peace of mind, but additional violence may not materialize; thus there may not be a reason to expend the resources this option requires.
- This course of action assumes that any violence will be directed against the embassy structure only and will not ignite broader unrest, which could still put staff in harm's way and cause the embassy to incur the cost of evacuation.

Step 6: Compare the Pros, including any Faults, against the Cons and Fixes.

See Table 17.8 for the full array of Pros, Cons, Faults, and Fixes.

Analytic Value Added: Based upon your assessment of the Pros and Cons, how can the United States best refine its strategy to protect its political and security interests in Belgrade? PCFF adds value by helping decision makers troubleshoot a given course of action. In this case, a simple administrative closure alone would most likely protect some, but not all, US interests. The technique identifies several steps and further points for consideration as the United States prepares for the coming week:

- The United States would be best served by accompanying an administrative closure with a series of diplomatic and security actions designed to prepare staff for a possible evacuation scenario, increase security and defenses around the embassy, and provide a means of egress should those defenses fail. These actions would include public and private diplomatic outreach to the Serbian government and a review of internal US planning and preparation for evacuation by the skeleton team if the riots resume and threaten the embassy.

The PCFF technique also helps to identify some underlying assumptions embedded in this option that deserve consideration and may, upon further discussion, influence the course of action:

- The first assumption is that the Serbs have both the ability and willingness to repel future attacks. While the Serbian riot police repelled the attackers on Sunday, they did so with some difficulty. Also, bilateral tensions rose significantly on Monday, when the United States recognized Kosovo's independence. While this does not mean that the Serbian government will abandon its Vienna Convention obligations, it could mean that the Serbs may be less

Table 17.8 ▶ Violence in Belgarade Pros-Cons-Faults-and-Fixes Example

Administrative Closure			
Faults	Pros	Cons	Fixes
The Serbs may not have the ability to manage an even larger rally than Sunday's, which could put US interests at risk. Given reports of a "secret plan" and the difficulty that Serb police had dispelling attackers on Sunday, it may not be safe to assume that the Serbs can manage the situation.	Diplomatically gives Serbs the benefit of the doubt that they have the willingness and ability to protect the embassy per their Vienna Convention obligations.	Assumes that the Serbs will adopt a proactive policy to protect the US embassy.	Reach out diplomatically in private to the Serbians, thanking them for Sunday's assistance and requesting/discussing strategy for cooperation in advance of Thursday's rally. Couple with public statements of tempered appreciation for Serb police assistance on Sunday and ongoing dialogue with Serb government.
Additional violence may not materialize; thus there may not be a reason to expend the resources.	Protects physical structure and personnel security by removing nonessential personnel from the premises and allowing the Marines to "batten down the hatches," rather than having the usual stream of employees and visitors in and out of the Chancery.	The embassy lacks a buffer between the building and the sidewalk/street, which makes it particularly vulnerable to attack.	Publicize Serb government's responsiveness to Sunday's attacks and ongoing dialogue between US and Serbian governments as a deterrent to would-be vandals and a message to Serbia that the United States expects proactive Serbian policing.
Assumes that any violence will be directed against the embassy structure only and will not ignite broader unrest, which could still put staff in harm's way and cause the embassy to incur the cost of evacuation.	This option is not without cost but is a relatively economical solution, given that the embassy can retain a skeleton staff with a Marine security detachment and quickly reopen with full staff once tensions dissipate.	If the closure is prolonged, it will reduce productivity, increase costs, and still put the core team and Marines at risk.	Better safe than sorry. Find a middle approach that protects US persons, policy, and information in embassy structure while minimizing economic impact. Develop a plan to protect any sensitive information (e.g., Iran in 1979) and an evacuation plan.

inclined to take a proactive approach to planning for Thursday's ostensibly peaceful rally.

- The second assumption that bears further consideration is that violence, should it occur, will only be directed against symbols of the United States and the West and not against US persons wherever they may be. As a result, it is important to plan for a total, rapid evacuation of the embassy.
- Lastly, there is an assumption that events will not ignite broader violence that could necessitate total evacuation. Reports of violence in Kosovo and additional riots on Monday in Belgrade suggest that additional planning is necessary for this possible scenario, especially during the administrative closure when the embassy staff are dispersed in their respective homes around the city.

CONCLUSION

In the face of growing fears about more looting and violence, on Wednesday, 20 February 2008, the United States announced an administrative closure of the US Chancery in Belgrade beginning at noon on Thursday, 21 February 2008, and continuing until Monday, 25 February 2008.[2,3] Only a core group of security and other officials would remain in the embassy. On Thursday, State Department spokesperson Sean McCormack told reporters that the department had spoken to the Serbian government about the latter's obligation to protect the embassy and noted that "they have been, up until this point, very good in providing police assets to ensure that the embassy facility was protected." McCormack added that "we are in contact with them, to make sure that they devote the assets to deal with the situation."[4]

That afternoon in Belgrade, over 150,000 people gathered at the old Yugoslav Parliament building for a government-supported rally to protest Kosovo's declaration of independence. Protesters waved Serbian flags and carried placards saying "Stop US Terror."[5,6] Koštunica delivered an impassioned speech in which he condemned Kosovo's secession, saying, "As long as we live, Kosovo is Serbia. Kosovo belongs to the Serbian people." After the rally, the crowd marched to the Temple of Saint Sava, Belgrade's largest church.[7]

Although there are different accounts of the exact numbers of rioters, at about 1900 hours, a crowd of 1,000 to

6,000 protesters broke away from the crowd of peaceful protesters and converged on the US and other pro-Kosovo embassies. At the time of the attack, press reports indicate that there was either no police presence at the US embassy building or that police withdrew when the crowd approached.[8,9,10,11] The attackers tore metal grills from windows, ripped the US flag from its pole, and broke a handrail off the entrance and used it to smash into the Chancery. Once inside, they threw furniture from the windows and set fire to the building, while the crowd outside shouted "Serbia, Serbia."[12,13,14,15] One protester died in the blaze.[16] According to a firsthand account by Master Sergeant John Finnegan of the Marine Security Guard Detachment, "There were too many [protesters] for the police to handle and a whole lot more were on the way. . . . The police couldn't help us out and [rioters] had free access to the embassy. We made the call to pull everybody back. We got everybody to a safe area and hunkered down."[17]

It reportedly took police between thirty and forty-five minutes to appear at the scene, and firefighters arrived at about the same time to put out the blaze. The protest lasted about two hours as police fought to disperse the crowd and secure the building using tear gas and armored cars.[18,19,20] The protesters also attacked the embassies of Bosnia-Herzegovina, Canada, Croatia, Germany, Slovenia, Turkey, and the United Kingdom.[21,22] In all, over 150 people were injured, nearly were 200 arrested, and 90 shops were ransacked.[23]

After the attack, the United States lodged a formal protest with the Serbian government, citing Serbia's Vienna Convention obligations. The White House spokesperson said the Chancery had been "attacked by thugs" and that Serbian police had not done enough to stop them.[24] State Department spokesperson Sean McCormack indicated that there was "not adequate security, either in numbers or capability, to prevent this breach of our embassy compound."[25] He noted, however, that the protesters did not breach the "so-called hard line," which is the secure area of the Chancery. [26]

In comments to the US Senate Armed Services Committee, Director of National Intelligence Mike McConnell said, "We have good information that when the US Embassy and the British Embassy and others were attacked, a decision was taken by the government of Serbia actually to pull the police back and allow them to be attacked, burn the embassy and conduct the violence they conducted."[27] A spokesperson for McConnell later clarified that the statement was based in part on eyewitness accounts and that there was no final conclusion or determination on this point, although he added, "I'm not going to say [eyewitness accounts were] the only thing" the director drew on in his remarks.[28]

The UN Security Council condemned the "mob attacks" and issued a unanimous statement noting the inviolability of diplomatic missions under international law and welcoming steps by Serbian authorities to restore order.[29]

Serbian Foreign Minister Jeremic called for an end to the protests, indicating that the violent acts were unacceptable and hurt Serbia's image abroad.[30] Koštunica issued a statement saying violence damaged Serbia's national interests, but he noted that the people of Serbia "have said what they think about Kosovo and the brutal violence Serbia is subjected to."[31] The Serbian minister responsible for Kosovo said the United States was to blame for the violence: "the Serbian government will continue to call on the US to take responsibility for violating international law and taking away a piece of territory from Serbia."[32]

Ultimately, the United States, citing unsafe conditions in Belgrade, evacuated nearly 100 nonessential staff and dependents out of Serbia via a forty-car convoy on Sunday 23 February, and the State Department did not authorize their return until 31 March.[33,34,35] The embassy remained closed to the public until 1 April 2008 as a result of extensive damage to the building.[36]

The Serbian senior prosecutor vowed to identify the culprits, and the Serbian government opened an investigation.[37] The results have not been made public.

For its part, the United States in 2010 broke ground on a new embassy facility on a twelve-acre site in a Belgrade suburb as part of a global effort to protect its foreign missions from attack. In a statement, the United States said that the new site in Belgrade will "provide safe, secure and functional facility for 400 employees who will work at the embassy."[38,39]

KEY TAKEAWAY

- In time-sensitive situations, there is often a tendency to allow the pressure of the moment to drive analysis toward the most obvious or convenient course of action. In this case, a decision merely to close the facility to the public—as several other Western countries chose to do—could have put more lives at risk if more than just the core team were in the building at the time of the attack. Decision Support techniques can slow down cognitive momentum in highly charged situations so that analysts and decision makers can fully consider the forces, factors, options, and angles that will shape the best decision.

NOTES

1. Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis,* 2nd ed. (Washington, DC: CQ Press, 2015, 102).
2. Charlie Coon and Kent Harris, "Marines at Embassy in Belgrade Hunker Down, Wait Out Crisis," *Stars and Stripes*, February 23, 2008, http://www.stripes.com/news/marines-atembassy-in-belgrade-hunker-down-wait-out-chaos-1.75379.
3. "US Embassy in Belgrade Attacked," BBC, February 22, 2008, http://news.bbc.co.uk/2/hi/7256158.stm.
4. Walter Pincus, "Serbia Withdrew Police, Intelligence Chief Says," *Washington Post*, February 28, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/02/27/AR2008022703383.html.
5. "US Embassy in Belgrade Attacked," BBC.
6. "Over 150 Injured in Belgrade Riots," RIA Novosti, February 22, 2008, http://en.rian.ru/world/20080222/99859211.html.
7. Ibid.
8. Ibid.
9. Pincus, "Serbia Withdrew Police, Intelligence Chief Says."
10. "Rioter Dies in Burning Embassy as Serbs Take to Streets over Kosovo," *Times* (London), February 22, 2008, http://www.timesonline.co.uk/tol/news/world/europe/article3413753.ece.
11. "State Department Briefs Press on Situation at US Embassy Belgrade," Federal News Service, February 21, 2009.
12. "US Embassy in Belgrade Attacked," BBC.
13. Pincus, "Serbia Withdrew Police, Intelligence Chief Says."
14. "Rioter Dies in Burning Embassy," *Times*.
15. "State Department Briefs Press on Situation at US Embassy Belgrade," Federal News Service.
16. "Rioter Dies in Burning Embassy," *Times*.
17. Coon and Harris, "Marines at Embassy in Belgrade Hunker Down, Wait Out Crisis."
18. "Rioter Dies in Burning Embassy," *Times*.
19. "US Embassy in Belgrade Attacked," BBC.
20. "State Department Briefs Press on Situation at US Embassy Belgrade," Federal News Service.
21. Z. Kusovac, "Kosovo Protest Leads to Violence in Belgrade," *Jane's Defence Weekly*, February 22, 2008.
22. Jovan Matic, "Belgrade Embassy Attacks Spark International Protests," Agence France Presse, *Sydney Morning Herald* (Australia), February 22, 2008, http://news.smh.com.au/world/belgrade-embassy-attacks-spark-international-protests-20080222–1tsa.html.
23. Coon and Harris, "Marines at Embassy in Belgrade Hunker Down, Wait Out Crisis."
24. "US Embassy in Belgrade Attacked," BBC.
25. "State Department Briefs Press on Situation at US Embassy Belgrade," Federal News Service.
26. Ibid.
27. Pincus, "Serbia Withdrew Police, Intelligence Chief Says."
28. Ibid.
29. "US Embassy in Belgrade Attacked," BBC.
30. "Rioter Dies in Burning Embassy," *Times*.
31. "Koštunica: Youth Show They Want Justice," Tanjug, February 22, 2008, http://www.b92.net/eng/news/politics-article.php?yyyy=2008&mm=02&dd=22&nav_id=47900.
32. "US Starts Evacuation from Serbia," BBC, February 23, 2008, http://news.bbc.co.uk/2/hi/europe/7260613.stm.
33. Ibid.
34. Dragana Jovanovic, "After Belgrade Attack, US Embassy Re-opens," *ABC News*, February 27, 2008, http://abcnews.go.com/International/story?id=4355835.
35. "United States Reopens Ransacked Belgrade Embassy," Reuters, March 31, 2008, http://uk.reuters.com/article/2008/03/31/us-serbia-us-embassy-idUKL313048120080331.
36. Ibid.
37. "US Starts Evacuation from Serbia," BBC.
38. Embassy of the United States Serbia, "US and Serbian Officials Break Ground for New Embassy Compound," February 10, 2010, http://serbia.usembassy.gov/bilateral20100210.html.
39. Embassy of the United States Serbia, "Contract Awarded for the Construction of the New US Embassy Compound," March 11, 2009, http://serbia.usembassy.gov/bilateral20090311.html.