

Sarah Miller Beebe
Randolph H. Pherson



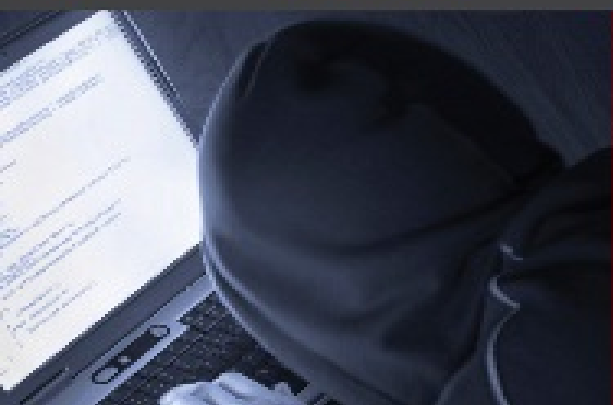
SECOND EDITION

Cases in Intelligence Analysis

STRUCTURED
ANALYTIC TECHNIQUES
IN ACTION



Foreword by Jack Davis





INVESTIGADOR_Z

INVESTIGADOR_Z

More Praise for *Cases in Intelligence Analysis*

“My students very much enjoyed using the case studies. They were real world, relevant, and helped bring the theory of Structured Analytic Techniques (SATs) into practice. One of my students said he wished he’d known about SATs ‘at the beginning of my college career,’ as he felt it helped him focus his thinking and decision making. I highly recommend it for faculty teaching about SATs and looking to improve critical thinking in general among their student population.”

—CDR Toni Gay
U.S. Coast Guard Academy
*Intelligence Studies Director and
Associate Professor 2009–2013*

“*Cases in Intelligence Analysis: Structured Analytic Techniques in Action* represents very deep analytical work, written with vision and experience that only true specialists can bring. I recommend it highly to new and experienced practitioners, instructors, and students alike. This excellent book fully supports the instruction of structured analytic techniques, and the step-by-step methodology is easy to follow. Thanks to Beebe and Pherson, SATs are forever going to be easier to teach and learn. A mandatory book for any intelligence analyst’s personal library.”

—Arturo Fuenzalida P.
Rear Admiral (Ret.)—Intelligence Analyst-Chilean Navy

“The best way to teach students how to analyze and interpret crucial events in international affairs, this indispensable set of cases should be required reading in every political science department. *Experto credite.*”

—Edward M. Roche, PhD, JD
Professor (Affil.), Grenoble Ecole de Management

“*Cases in Intelligence Analysis* is a must-have practical text for intelligence practitioners and serious students of the field. With its companion text, *Structured Analytic Techniques for Intelligence Analysis*, by Richards J. Heuer Jr. and Randolph H. Pherson, the book masterfully guides readers through some of the most important analytical concepts and challenges. Its case studies, each clearly written and accessible, stimulate thinking beyond the instinctive guesswork of much traditional analysis into the sophisticated but satisfying realm of structured techniques. Its authors have made another significant contribution to the development of the discipline.”

—Michael Mulqueen, PhD
*Associate Professor and Head of the Department of Politics, History, Media, and
Communication, Liverpool Hope University, England*

“This text really draws students in—allowing them to go beyond merely reading and learning

about intelligence to actually using techniques to analyze real-life intelligence cases. Students are engaged by the material, which works well for both on-campus and online courses.”

—Mary Manjikian, PhD
Regent University

“The book is well written and stimulating on a number of levels. It provides students with insights into the real-world issues confronting intelligence analysts as they attempt to make sense of often conflicting and complex data and information related to the cases.”

—Jonathan Benjamin-Alvarado, PhD
University of Nebraska Omaha

Cases in Intelligence Analysis

Structured Analytic Techniques in Action

Second Edition

Sarah Miller Beebe
Randolph H. Pherson

 **SAGE** | 
CQ PRESS

Los Angeles | London | New Delhi
Singapore | Washington DC

Copyright © 2015 by CQ Press, an Imprint of SAGE Publications, Inc. CQ Press is a registered trademark of Congressional Quarterly Inc.

All rights reserved. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

Printed in the United States of America

Library of Congress Cataloging-in-Publication Data

Beebe, Sarah Miller.

Cases in intelligence analysis : structured analytic techniques in action / Sarah Miller Beebe and Randolph H. Pherson.—Second edition

pages cm

Includes bibliographical references (p.).

ISBN 978-1-4833-4016-6 (alk. paper)

1. Intelligence service—Methodology—Case studies. I. Pherson, Randolph H. II. Title.

JF1525.I6B44 2015

327.12—dc23

2014000289

14 15 16 17 18 10 9 8 7 6 5 4 3 2 1

INVESTIGADOR_Z



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 1/1 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.
Copy Editor: Pam Suwinsky
Proofreader: Talia Greenberg
Cover Designer: Edgar Abarca
Interior Graphics Designer: Adriana M. Gonzalez
Marketing Manager: Amy Whitaker

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

To Richie and Amanda—the next generation.

INVESTIGADOR_Z

Brief Contents

Annotated Contents

Tables, Figures, and Boxes

Matrix of Techniques

Foreword to the Second Edition

BY JACK DAVIS, CIA TRAILBLAZER

Foreword to the First Edition

BY ROBERT JERVIS, COLUMBIA UNIVERSITY

Preface

About the Authors

INTRODUCTION

1 WHO POISONED KARINNA MOSKALENKO?

Case Narrative

Who Poisoned Karinna Moskalenko? Structured Analytic Techniques in Action

2 THE ANTHRAX KILLER

Case Narrative

The Anthrax Killer: Structured Analytic Techniques in Action

3 CYBER H₂O

Case Narrative

Cyber H₂O: Structured Analytic Techniques in Action

4 IS WEN HO LEE A SPY?

Case Narrative

Is Wen Ho Lee a Spy? Structured Analytic Techniques in Action

5 JOUSTING WITH CUBA OVER RADIO MARTI

Case Narrative

Jousting with Cuba over Radio Marti: Structured Analytic Techniques in Action

6 THE ROAD TO TARIN KOWT

Case Narrative

The Road to Tarin Kowt: Structured Analytic Techniques in Action

7 WHO MURDERED JONATHAN LUNA?

Case Narrative

Who Murdered Jonathan Luna? Structured Analytic Techniques in Action

8 THE ASSASSINATION OF BENAZIR BHUTTO

Case Narrative

The Assassination of Benazir Bhutto: Structured Analytic Techniques in Action

9 DEATH IN THE SOUTHWEST

Case Narrative

Death in the Southwest: Structured Analytic Techniques in Action

10 THE ATLANTA OLYMPICS BOMBING

Case Narrative

The Atlanta Olympics Bombing: Structured Analytic Techniques in Action

11 THE DC SNIPER

Case Narrative

The DC Sniper: Structured Analytic Techniques in Action

12 COLOMBIA'S FARC ATTACKS THE US HOMELAND

Case Narrative

Colombia's FARC Attacks the US Homeland: Structured Analytic Techniques in Action

13 UNDERSTANDING REVOLUTIONARY ORGANIZATION 17 NOVEMBER

Case Narrative

Understanding Revolutionary Organization 17 November: Structured Analytic Techniques in Action

14 DEFENDING MUMBAI FROM TERRORIST ATTACK

Case Narrative

Defending Mumbai from Terrorist Attack: Structured Analytic Techniques in Action

15 IRANIAN MEDDLING IN SAUDI ARABIA

Case Narrative

Iranian Meddling in Bahrain: Structured Analytic Techniques in Action

16 SHADES OF ORANGE IN UKRAINE

Case Narrative

Shades of Orange in Ukraine: Structured Analytic Techniques in Action

17 VIOLENCE ERUPTS IN BELGRADE

Case Narrative

Violence Erupts in Belgrade: Structured Analytic Techniques in Action

Image Credits

Annotated Contents

Tables, Figures, and Boxes

Matrix of Techniques

Foreword to the Second Edition

BY JACK DAVIS, CIA TRAILBLAZER

Foreword to the First Edition

BY ROBERT JERVIS, COLUMBIA UNIVERSITY

Preface

About the Authors

INTRODUCTION

1 WHO POISONED KARINNA MOSKALENKO?

*The poisoning of prominent Russian human rights lawyer Karinna Moskalenko captured worldwide media attention in the fall of 2008. It was regarded as yet another entry in a growing list of poisonings and assassinations alleged carried out by Russia's government against its critics at home and abroad. The case employs the **Premortem Analysis**, **Structured Self-Critique**, and **Starbursting** techniques to help analysts examine the facts of this fast-moving story and develop a robust set of questions to guide a nuanced analysis of the case.*

Case Narrative

Who Poisoned Karinna Moskalenko? Structured Analytic Techniques in Action

2 THE ANTHRAX KILLER

*On 15 October 2001, a fine white substance poured out of a letter opened by a clerk intern in Sen. Tom Daschle's office on Capitol Hill. By the end of the day the white powder was confirmed to be a deadly dose of anthrax. Over the ensuing weeks, cases of anthrax emerged in Connecticut, Florida, Washington, D.C., New Jersey, and New York. The incident riveted the attention of the nation: Who could be behind the attack, and how far might it spread? In this case, **Chronologies** frame the problem and bring order to the jumble of data points; **Timelines** put key facts and events in context; and a **Premortem Analysis** and **Structured Self-Critique** help illuminate important areas for further consideration by developing alternative explanations, challenging assumptions, identifying biases, and closely examining the evidentiary base.*

INVESTIGADOR_Z

Case Narrative

The Anthrax Killer: Structured Analytic Techniques in Action

3

CYBER H₂O

*On 8 November 2011 at the Curran-Gardner Public Water District just outside Springfield, Illinois, a large water pump repeatedly and spontaneously powered on and off. It was as if someone was repeatedly flipping an on/off switch. Although the pump had been behaving strangely for two or three months, it had never turned on and off repeatedly. By the end of the day the pump burned out, leaving it unusable. Utility officials were flummoxed. Who or what had caused the pump failure? The **Getting Started Checklist**, **Key Assumptions Check**, and **Devil's Advocacy** are quick and effective techniques that help analysts focus on the relevant questions, consider alternative outcomes, reveal unsupported assumptions, and troubleshoot their final analysis.*

Case Narrative

Cyber H₂O: Structured Analytic Techniques in Action

4

IS WEN HO LEE A SPY?

*In 1999, the New York Times reported that China had used stolen US nuclear secrets to make rapid advances in its nuclear warhead development. Given the small community of US scientists with access to such data, investigators quickly focused their case on Taiwanese American nuclear scientist Wen Ho Lee. Had Wen Ho Lee engaged in undetected nefarious activities for decades, or did the government narrow its gaze too quickly? Analysts use the **Force Field Analysis**, **Deception Detection**, **Premortem Analysis**, and **Structured Self-Critique** techniques to evaluate both sides of the case, test for deception, and troubleshoot the government's position that Wen Ho Lee was a spy.*

Case Narrative

Is Wen Ho Lee a Spy? Structured Analytic Techniques in Action

5

JOUSTING WITH CUBA OVER RADIO MARTI

By the time Ronald Reagan became president in 1981, the United States and Cuba had been engaged in diplomatic, economic, and armed conflict since Fidel Castro came to power in 1959. During its first year, the Reagan administration announced plans to begin broadcasting news of Cuba to Cubans from a radio station in Florida. The hope was that the radio broadcasts would challenge the Cuban regime's control of information on the island. It would also be part of the administration's strategy of directly confronting Cuba—an ally of the Soviet Union.

When Radio Marti—named after Cuban writer and national revolutionary hero Jose Marti—began broadcasting in May 1985, its low-key opening words

*“Buenos dias, Cuba” did not reflect the four years of uncertainty within the U.S. government about how Cuba would respond to broadcasts from a radio station intended as another American challenge to the Castro regime. Those four years would involve sophisticated Cuban efforts to influence the U.S. political process. Both countries would engage in threats and make counterthreats. The full range of intelligence collection and analysis including open source, human, and technical collection efforts would be employed. Cuba would conduct sophisticated counterintelligence measures. Finally, the United States would respond by developing a comprehensive set of countermeasures enabled by its technical and military capabilities should the Cubans retaliate when Radio Marti eventually started to broadcast. This case study applies **Chronologies and Timelines, Deception Detection, Quadrant Hypotheses Generation, and Analysis of Competing Hypotheses** to track the tactical moves and strategies employed by both countries and assess whether events were leading up to a radio war with Cuba.*

Case Narrative

Jousting with Cuba over Radio Marti: Structured Analytic Techniques in Action

6

THE ROAD TO TARIN KOWT

*The US military in 2005 faced a pivotal decision about building a paved road through a Taliban stronghold to Tarin Kowt, a provincial capital in Afghanistan. The United States and other international donors saw the road as a critical element in efforts to stabilize, modernize, and democratize Afghanistan. With Afghanistan’s first parliamentary elections since the overthrow of the Taliban on the horizon, the US Army considered embarking on a highly accelerated schedule to complete the road in time for the election. This case uses the **Kahn Assumptions Check, Devil’s Advocacy, and Strengths-Weaknesses Opportunities-Threats** techniques to structure a thorough assessment of the operating environment, the probable enemy response, and the potential impact on broader US goals for Afghanistan.*

Case Narrative

The Road to Tarin Kowt: Structured Analytic Techniques in Action

7

WHO MURDERED JONATHAN LUNA?

*Jonathan Luna was a youthful and gregarious federal prosecutor whose mysterious death in December 2003 shocked his friends and colleagues and led to a multiyear, multistate investigation into how and why Jonathan Luna died. With multiple theories swirling amid a plethora of ambiguous and sometimes contradictory evidence, analysts use **Chronologies and Timelines, Simple Hypotheses, the Multiple Hypotheses Generator™, and Analysis of Competing Hypotheses** to track and assess events, develop a range of plausible*

explanations, and rigorously evaluate evidence in this perplexing case.

Case Narrative

Who Murdered Jonathan Luna? Structured Analytic Techniques in Action

8

THE ASSASSINATION OF BENAZIR BHUTTO

*The assassination of Benazir Bhutto—Pakistan’s first female prime minister—during a political rally to support her presidential candidacy in 2007 sent shock waves through the international community and generated a wave of accusation and counteraccusations about who was responsible. Despite a lengthy investigation, questions remain about who was behind the assassination. This case employs **Chronologies and Timelines** to help analysts assemble the evidence and identify information gaps, a **Mind Map** to help them think creatively about possible perpetrators, and **Analysis of Competing Hypotheses** to assist in their evaluation of a range of possible explanations.*

Case Narrative

The Assassination of Benazir Bhutto: Structured Analytic Techniques in Action

9

DEATH IN THE SOUTHWEST

*In the spring of 1993, residents of the Four Corners area of the US Southwest started dying rapidly and unexpectedly. Doctors at first suspected virulent flu but they were flummoxed by inconclusive test results and the high mortality rate of their patients. With little solid data available, they faced a daunting and urgent diagnostic challenge. This case uses **Structured Brainstorming** to help analysts think creatively and exhaustively about the possible cause, **Starbursting** to organize that thinking around key questions, the **Multiple Hypotheses Generator™** to create a full range of alternative hypotheses, and **Key Assumptions Check** and **Analysis of Competing Hypotheses** to scrutinize the evidence and narrow the range of most likely explanations.*

Case Narrative

Death in the Southwest: Structured Analytic Techniques in Action

10

THE ATLANTA OLYMPICS BOMBING

*After a bomb ripped through the crowd at the 1996 Olympics Centennial Parade killing one person and injuring 111, authorities began a furious search for those responsible for the attack. An erstwhile security guard who had previously warned authorities about the suspicious package quickly emerged as the chief suspect in the case. A **Key Assumptions Check** helps analysts evaluate the course of action taken by the authorities as they began the case, **Pros-Cons-Faults-and-Fixes** provides analysts with a framework to assess the evidence for and against*

the main suspect, and the **Multiple Hypotheses Generator™** assists identifying other plausible perpetrators of the crime.

Case Narrative

The Atlanta Olympics Bombing: Structured Analytic Techniques in Action

11

THE DC SNIPER

*In 2002, only a year after the 9/11 attacks, Washington, D.C., was again gripped with fear as men, women, and children were gunned down by sniper fire across the greater metropolitan area. As authorities raced to find the culprit, they were inundated with myriad eyewitness reports, call-in tips, and other data, but assessing this information proved difficult. This case uses a **Key Assumption Check** to help analysts uncover and challenge implicit assumptions that color evaluation of the available evidence, and it employs the **Multiple Hypotheses Generator™** and **Classic Quadrant Crunching™** to help systematically develop and assess a range of possible explanations.*

Case Narrative

The DC Sniper: Structured Analytic Techniques in Action

12

COLOMBIA'S FARC ATTACKS THE US HOMELAND

*The Revolutionary Armed Forces of Colombia (FARC) is Latin America's largest, oldest, and most capable insurgent group. Its history of kidnapping, assassinations, and indiscriminate acts of violence makes it one of the most despised groups in Colombia, but it has never conducted operations in the United States. This case helps analysts to assess the possibility of such an attack against the homeland using **Red Hat Analysis**, **Structured Brainstorming**, **Multiple Scenarios Generation**, **Indicators**, and the **Indicators Validator™** to prompt creative thinking about the range of possible FARC attack scenarios and to identify specific signs that would tip off local officials of an impending attack.*

Case Narrative

Colombia's FARC Attacks the US Homeland: Structured Analytic Techniques in Action

13

UNDERSTANDING REVOLUTIONARY ORGANIZATION 17 NOVEMBER

In 1975, the CIA's most senior official assigned to Athens, Greece—Chief of Station Richard Welch—was killed by a previously unknown violent extremist group, Revolutionary Organization 17 November (17N). Over the course of the next three decades, 17N targeted and killed more than two dozen individuals including Greek, US, British, and Turkish political figures, diplomats, military officers, and prominent business people. It also caused millions of Euros in property damage through bombings and rocket attacks. Yet not a member of the

group was firmly identified or apprehended until 2002. This case study applies **Simple Hypothesis Generation**, **Foresight Quadrant Crunching™**, and **What If? Analysis** techniques to assess the nature of this elusive group and evaluate the scope of the threat it presented during its years of activity.

Case Narrative

Understanding Revolutionary Organization 17 November: Structured Analytic Techniques in Action

14

DEFENDING MUMBAI FROM TERRORIST ATTACK

In 2008, the United States quietly passed intelligence to the Indian government warning of Pakistani-based terrorist plans to attack hotels and business centers in Mumbai. It fell to Indian intelligence and law enforcement officials to identify the most likely timing, targets, and modes of attack. **Structured Brainstorming**, **Red Hat Analysis**, **Classic Quadrant Crunching™**, **Indicators**, and the **Indicators Validator™** help analysts evaluate most likely modes of transport, anticipate likely targets and credible attack scenarios, and recognize the signs that a particular scenario is beginning to take shape.

Case Narrative

Defending Mumbai from Terrorist Attack: Structured Analytic Techniques in Action

15

IRANIAN MEDDLING IN BAHRAIN

In April 2011, Bahrain sent a confidential report to the UN secretary general accusing Iran of using Hezbollah to support and possibly finance the Bahraini opposition's Arab Spring uprising. Iran rejected the accusation, and the opposition issued counterclaims against Bahrain's government. In the face of these conflicting claims and counterclaims, observers and analysts were left to navigate the sea of facts and allegations about Iranian meddling. The ramifications for the United States were significant: If Bahraini government claims were true, US policy had to address the prospect of a proxy war between Iran and Saudi Arabia; if opposition counterclaims and Iranian denials were true, US policy would focus on how domestic reforms might address opposition grievances. **Starbursting** helps identify key questions in the case, **Morphologic Analysis** explores possible alternatives for the claims and counterclaims, **Structured Brainstorming** explicates the key dimensions of the problem, and **Indicators** guide future collection and analysis.

Case Narrative

Iranian Meddling in Bahrain: Structured Analytic Techniques in Action

16

SHADES OF ORANGE IN UKRAINE

*As Ukraine's long winter melted into spring in 2004, Ukrainian politics heated up with the announcement of presidential elections for the fall. The U.S. relationship with the ruling party in Kiev was arguably at the lowest point since Ukraine's independence in 1991, and the election outcome could have serious consequences for US policy in the region. Would Ukraine's pro-US opposition have a chance of success against the combined efforts of Ukraine's wealthiest and most powerful political forces? **Structured Brainstorming**, **Outside-the-Box Thinking**, and **Simple Scenarios** help analysts to identify the key factors at play and explain how their dynamics could result in a range of possible futures.*

Case Narrative

Shades of Orange in Ukraine: Structured Analytic Techniques in Action

17

VIOLENCE ERUPTS IN BELGRADE

*A mob of angry protesters attacked the US Embassy compound in Belgrade in February 2008, causing limited damage to the building façade. Violence in the Serbian capital, coupled with sporadic eruptions in neighboring Kosovo, forced US officials to make difficult assessments about the prospective threat to U.S. interests in the region and how the United States should respond. Did the attacks presage greater violence against Americans, and should US officials count on Serbian authorities to protect the US diplomatic presence? **Force Field Analysis**, a **Decision Matrix**, and **Pros-Cons-Faults-and-Fixes** provide a robust framework for conducting a thorough assessment to support decision making in a crisis environment.*

Case Narrative

Violence Erupts in Belgrade: Structured Analytic Techniques in Action

Image Credits

Tables, Figures, and Boxes

Figure 1.1	Chronology of Alleged Russian Poisonings, 2000–2010
Figure 1.2	Chronology of the Karinna Moskalenko Poisoning
Table 1.1	Case Snapshot: Who Poisoned Karinna Moskalenko?
Table 1.2	Common Analytic Pitfalls
Figure 1.3	Starbursting Template
Table 2.1	Case Snapshot: The Anthrax Killer
Table 2.2	Common Analytic Pitfalls
Map 3.1	Location of the Curran-Gardner Public Water District Facility
Figure 3.1	Physical, Cyber, and Human Components of Water Utilities
Figure 3.2	Water Sector Interdependencies
Box 3.1	Lexicon of Cyber Attacks
Table 3.1	Case Snapshot: Cyber H ₂ O
Table 3.2	Key Assumptions Check Template
Figure 4.1	Schematic of the W-88 Nuclear Warhead
Table 4.1	Case Snapshot: Is Wen Ho Lee a Spy?
Table 4.2	Force Field Analysis Template
Table 4.3	When to Use Deception Detection
Table 4.4	Deception Detection Templates
Figure 5.1	Cuban Capabilities to Disrupt US Radio Broadcasting
Table 5.1	Case Snapshot: Jousting with Cuba over Radio Marti
Table 5.2	When to Use Deception Detection
Table 5.3	Deception Detection Templates
Figure 5.2	Quadrant Hypothesis Generation Template
Table 6.1	Tenets of Pashtunwali
Box 6.1	Soviet Lessons Learned
Map 6.1	Pashtun Tribal Areas and Insurgent Strongholds
Table 6.2	Afghan Ministries with Responsibilities for Roads, 2004–2005
Map 6.2	Route between Kandahar and Tarin Kowt
Table 6.3	Case Snapshot: The Road to Tarin Kowt
Table 6.4	Key Assumptions Check Template
Table 6.5	SWOT Template

Table 6.6	SWOT Second-Stage Analysis Template
Map 7.1	Jonathan Luna's Home, Work, and Location of Body
Table 7.1	Case Snapshot: Who Murdered Jonathan Luna?
Map 8.1	Pakistan
Figure 8.1	Communications Intercept Released by the Pakistani Government
Table 8.1	Case Snapshot: The Assassination of Benazir Bhutto
Map 9.1	Four Corners Region
Table 9.1	Diseases Transmitted by Rodents
Table 9.2	Case Snapshot: Death in the Southwest
Box 9.1	Eight Rules for Successful Brainstorming
Figure 9.1	Starbursting Template
Table 9.3	Key Assumptions Check Template
Map 10.1	Centennial Park
Figure 10.1	Bomb Specifications and ALICE Pack
Table 10.1	Case Snapshot: The Atlanta Olympics Bombing
Table 10.2	Key Assumptions Check Template
Table 10.3	Pros-Cons-Faults-and-Fixes Template
Table 10.4	Multiple Hypotheses Generator™ Template
Figure 11.1	Tarot Card Found at Site of Iran Brown Shooting
Figure 11.2	FBI Profile of DC Sniper
Figure 11.3	First Page of Letter Found at Ponderosa Steak House
Map 11.1	Locations of the Sniper Shootings in the Washington, D.C., Region
Table 11.1	Case Snapshot: The DC Sniper
Table 11.2	Key Assumptions Check Template
Table 11.3	Multiple Hypotheses Generator™ Template
Table 11.4	Classic Quadrant Crunching™ Matrix Template
Map 12.1	FARC Presence in Colombia and Coca Cultivation Areas
Figure 12.1	Chronology of Key Events in Colombia
Table 12.1	US Military Support to Colombia
Table 12.2	Case Snapshot: Colombia's FARC Attacks the US Homeland
Box 12.1	Tensions Mount: A Future Scenario
Box 12.2	Eight Rules for Successful Brainstorming
Table 13.1	Timeline of Significant 17N Attacks
Table 13.2	Case Snapshot: Understanding Revolutionary Organization 17 November
Table 13.3	Foresight Quadrant Crunching™ Template

Map 14.1	Mumbai Peninsula
Table 14.1	Bomb Blasts in Mumbai, 1993–2008
Box 14.1	RDX Bombs
Map 14.2	India, Mumbai, and Previous Attack Sites
Table 14.2	Case Snapshot: Defending Mumbai from Terrorist Attack
Box 14.2	Eight Rules for Successful Brainstorming
Table 14.3	Classic Quadrant Crunching™ Matrix Template
Map 15.1	Bahrain from a Regional Perspective
Table 15.1	Distinctions between Bahraini and Iranian Shias
Table 15.2	Examples of Iranian Influence in the Middle East
Table 15.3	Bahraini Opposition Members Arrested on 17 March 2011
Table 15.4	Case Snapshot: Iranian Meddling in Bahrain
Figure 15.1	Starbursting Template
Table 15.5	Morphological Analysis Template
Box 15.1	Eight Rules for Successful Brainstorming
Box 16.1	Kuchma's Proposed Constitutional Changes
Figure 16.1	The Rada and the Constitutional Court Split, 18 March 2004
Map 16.1	Ukraine
Box 16.2	Ukraine through Russian Eyes
Box 16.3	Georgia's "Rose Revolution"
Figure 16.2	2004 Ukrainian Presidential Election Players and Parties
Table 16.1	Case Snapshot: Shades of Orange in Ukraine
Box 16.4	Eight Rules for Successful Brainstorming
Table 16.2	Simple Scenarios Template
Map 17.1	Serbia and the Breakaway Republic of Kosovo
Figure 17.1	February 2008: Kosovo Status at an Impasse
Box 17.1	Protecting US Diplomatic Missions
Figure 17.2	Chronology of Selected Events
Table 17.1	Case Snapshot: Violence Erupts in Belgrade
Table 17.2	Force Field Analysis Template
Table 17.3	Decision Matrix Template
Table 17.4	Pros-Cons-Faults-and-Fixes Template

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 IFT ANALYSIS	DEVIL'S ADVOCACY	DECISION MATRIX	FORCE FIELD ANALYSIS	PROS-CONS-FAULTS-FIXES	STRENGTHS, WEAKNESSES, OPPORTUNITIES, THREATS	
1. Who Poisoned Karinna Moskalenko?				❖	◆													❖				◆	◆						
2.The Anthrax Killer		◆		❖														❖				◆	◆						
3. Cyber H ₂ O	◆																							◆					
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. 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.

Foreword to the First Edition

Robert Jervis, Columbia University

Ever since Roberta Wohlstetter's pathbreaking study of why the United States was taken by surprise at Pearl Harbor fifty years ago,¹ both academics and members of the Intelligence Community (IC) have made significant progress in understanding intelligence failures. About how to correct these errors and do better we know much less, however, and it is to this subject that this volume makes a major contribution.

The fundamental problem, still unrecognized by most members of the general public and all too many government officials, is that intelligence can never be right all the time, even on the most important issues on which it concentrates the bulk of its resources. Others have said this better than I, so let me just draw on two quite different observers. Clausewitz saw that "many intelligence reports in war are contradictory; even more are false, and most are uncertain."² The only amendment I would make is to drop the modifier "in war." Samuel Butler put it even more broadly: "Life is the art of drawing sufficient conclusions from insufficient premises."³ The world is too complex, evidence is too fragmentary and inconsistent, and our brains and organizations are too limited to allow us to completely understand the world and accurately discern others' capabilities and intentions. Indeed, in addition to the evidence being convoluted and often contradictory, people and states often behave in ways that are inconsistent (even leaving aside the fact that they and those who are trying to understand them may define *consistency* very differently).

In international politics, furthermore, deception is rampant. Adversaries usually wish to mislead others about at least some aspects of what they can and will do. Those who expect intelligence services to ferret out the truth should remember how often one—or even both—members of a couple are startled to eventually learn about the other's infidelity. In an additional nasty twist, the knowledge that deception is possible degrades valid information (something that can happen in marriages as well). One reason American intelligence was not disturbed by the paucity of solid evidence that Saddam Hussein's Iraq was actively pursuing weapons of mass destruction (WMD) was the well-founded (but later proven incorrect) belief that it was employing an extensive deception and denial program.⁴

Deception sometimes adds to and sometimes competes with the enormous amount of misleading information that is generated in the natural course of events—the "noise" that disguises "signal," to use Wohlstetter's terms. Many items of information are true but not diagnostic. And often remarks by a foreign leader may tell us quite a bit, but then again they may not—they may be exceptions or aberrations; in other cases, the remarks may have been intended for domestic audiences, or they may have represented designs that were later abandoned or the views of the faction that did not prevail. Even apparently solid evidence may not be so. Iraq

seemed to be building plants that produced potentially dangerous chemicals in amounts far in excess of the civilian needs, but it turned out that the country did need the products for innocent use.

Most evidence is then highly ambiguous. This makes our lives very difficult, both as individuals and as intelligence analysts. In fact, it would make our lives impossible if we were to form our conclusions only on the basis of particular bits of information as they are received. To act in a world filled with messy information, we have to come to conclusions fairly quickly, not be swayed by every stray bit of information that comes our way, and have the beliefs and theories that we have formed (partly on the basis of information) guide what we see and how we see it. This way of thinking may seem unempirical, unfair, and indefensible. It implies we are closed-minded and impervious to annoying facts. So we fail to understand that this is the way that we *do* think and, instead, believe that we are being fair to all the facts, which actually is impossible. We may think that it is a bit too suspicious to say, “I’ll believe it when I see it,” but few doubt that this is the right approach. But this is not the way we think, and cannot be.

Closer to the truth is to say, “I’ll see it when I believe it.” Our minds are hardwired to make sense out of disparate goings-on, to see patterns and cause-and-effect relations in our environment, and to quickly make sense out of things. We probably could not survive as individuals or as a species otherwise; our ancestors would quickly have been devoured by predators had they not jumped to the conclusion that the rustling in the bushes might be a saber-toothed tiger. But the result is that when the picture that we have in our mind is wrong, the interpretation of evidence that we make, often easily and quickly, will not only be consistent with this picture but will reinforce the error. Indeed, alternative interpretations may be almost impossible unless we already have an alternative perspective.

Iraq again provides a telling example. In his speech to the United Nations, Secretary of State Colin Powell quoted Baghdad as telling officials at a military base that was about to be visited by the US inspectors: “We sent you a message...to clean out all the areas, the scrap areas, the abandoned areas. Make sure there is nothing there.” The meaning seems—or seemed—self-evident. Now we know that it was not, and that the Iraqis were just seeking to remove signs or bits of evidence that would in fact have been misleading. But as far as I know, no one suggested this at the time, even though in retrospect the specifying of “the scrap areas, the abandoned areas” could have been correctly read as indicating a fear that traces of old chemicals remained even though the weapons had been destroyed.

The reason was that almost no one understood Saddam’s bizarre approach and outlook. More afraid of Iran, domestic opponents, and his own generals, he played a bizarre form of bluff. Compounded by the rivalries, corruption, and inefficiencies that characterized the regime, this made sense of a good deal (although not all) of the evidence. But one could not interpret the evidence in this way until one had first grasped what Saddam’s regime was all about.⁵

Intelligence analysis then tries to make sense of the world, and it can only produce intelligible reports when analysts have some idea of what they are seeing. No analysts can be “true to all the facts”—not only is what constitutes a fact not objective, but many “facts” actually prove to be false. Ignoring them, or at least putting them aside, is a necessary part of the human endeavor; it is not antiscientific. To take just one example, recently scientists reported that meticulous analysis found particles traveling faster than the speed of light. If this is true, Einstein’s laws of relativity must be thrown out. Doing so means discarding much of modern physics, and because that has been supported by so much theory and evidence, almost all scientists assume that the recent finding will eventually be shown to be mistaken.

Good scientists then are closed-minded—at least to a point. But it is impossible to specify rules by which we can tell that this point has been passed. In numerous battles over intelligence, each side thinks the other is being preposterously stubborn and for reasons of ego, politics, or worldview is sticking to a discredited hypothesis in the face of massive evidence to the contrary. Someone is right, but usually both sides are reasoning in a similar manner, and after the fact we often can continue the debate. Thus, while most people believe that there were no strong connections between Saddam's regime and terrorists, especially al-Qaeda, and that analysts in the Office of the Secretary of Defense and the Office of the Vice President both clutched at straws and greatly exaggerated, if not lied, others claim that they were right and it is those who denied these links who were unprofessionally closed-minded.⁶

This is bad enough, but it gets even worse. Intelligence analysis, like other forms of understanding the world, is most convincing when it is most plausible in the sense of seeming to fit best not only with specific bits of evidence but with the general sense of how people and states behave that we have built up over the years. Almost by definition, this serves us well in most cases. But it makes us ill suited to detect change or exceptions. Richard Betts shows that it is in just these circumstances that intelligence is particularly likely to go wrong.⁷ The problem is not that we are overlooking facts, are too closed-minded, or are under great political pressure, although these forces are troublesome and can be present. But even when they are not, it is very hard to understand what others are doing when a correct answer does not make much sense. Sometimes the problem is that we are mirror imaging and projecting our goals and beliefs onto others, sometimes others are being more clever than we are, and sometimes (as I believe is the case for Saddam) what others are doing is foolish and self-defeating. In all these cases, we will be misled.

Combating these and other impediments to good analysis is extraordinarily difficult. People have to be trained to think in counterintuitive ways. This is true in natural and social science as well, which is why my colleagues and I devote much of our teaching to forms (note the plural) of scientific reasoning in the treatment of evidence, something we would not need to do if this came naturally. But being aware of these problems, although an important step, is often insufficient.⁸

We need help, both as individuals and as organizations. And this is where *Cases in Intelligence Analysis* comes in. There have been other explications of structured analytic techniques, but they are hard to grasp in the abstract. Here they are brought to bear on specific cases. What is particularly telling is that when one reads several of the cases, some answers are likely to come too quickly to mind. These are very hard to shake, even though they are often wrong. I doubt if I am alone in thinking that I could not shake them intuitively. Rather, we need a set of tools to encourage or even force us to think about alternatives, to probe the evidence more deeply, to ask whether it really fits our conclusion and, even more, whether it contradicts alternative claims, and to think systematically about the next stages of our investigation. The cases are also interesting because when the mind does not immediately leap to a conclusion, the right answer—assuming there is one—is not obvious, and knowing the truth is a major barrier to fruitful thinking when we do most postmortems. Of course, there is no guarantee that these or other methods will lead us to the correct answer, even when there is one. Indeed, the techniques are disruptive, and that is their point.

Finally, we should note that it is not only analysts but intelligence consumers who may find the results disturbing. Policies are often built on intelligence and, in other cases, may produce confirming intelligence.⁹ In any case, although coming up with new and even better ideas is

appealing to academics, and occasionally to journalists, it is usually upsetting to policy makers. Policy is hard enough to establish; it is even more difficult to change. This assumes, of course, that better intelligence will come up with an answer that is better, if not exactly right. This will sometimes be the case, but even more annoyingly, better analytical techniques are likely to open minds to new alternatives without clearly indicating which one is correct.

Just as better intelligence on Iraq would have made policy makers less certain of Saddam's capabilities (assuming policy makers listened), so in many other cases good intelligence will ask them to think about several possibilities. This can be unsettling, especially to those with low tolerance for ambiguity. Better intelligence then requires strong policy makers who will not jump to conclusions but will be able to think about alternatives and ambiguities and nevertheless act as best they can.

This is a tall order, and helps explain why the policy-making community has not adequately pressed for a better intelligence system. The IC then has to look within its own resources to improve, and learning how to employ structured analytic techniques is a big step in the right direction.

NOTES

1. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962).
2. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 117.
3. Samuel Butler, *The Notebooks of Samuel Butler: Selections*, ed. Henry Festing Jones (London: A. C. Fifield, 1918), 11.
4. For more on this and other topics touched on here, see Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2010).
5. For fascinating evidence, see Kevin M. Woods, David D. Palkki, and Mark E. Stout, eds., *The Saddam Tapes: The Inner Workings of a Tyrant's Regime, 1978–2001* (New York: Cambridge University Press, 2011). This is not to say that there is agreement on the regime's motives, behavior, or likely course of actions had the United States allowed it to continue. As every historian knows, the passage of time and the opening of new archives does not always—or even usually—produce consensus.
6. See, for example, Christina Shelton, "The Roots of Analytic Failures in the U.S. Intelligence Community," *International Journal of Intelligence and CounterIntelligence* 24, no. 4 (2011): 337–55.
7. Richard K. Betts, "Theory Traps: Expertise as an Enemy," chap. 3 in *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007).
8. See the discussions of "de-biasing" and its limits: Philip E. Tetlock and Jae Il Kim, "Accountability and Judgment Processes in a Personality Prediction Task," *Journal of Personality and Social Psychology* 52, no. 4 (1987): 700–709; Tetlock, "Cognitive Biases and Organizational Correctives: Do Both Disease and Cure Depend on the Political Beholder?" *Administrative Science Quarterly* 45, no. 2 (2000): 293–326; Tetlock, "Social Functionalist Frameworks for Judgment and Choice: Intuitive Politicians, Theologians, and Prosecutors," *Psychological Review* 109, no. 3 (2002): 451–71. For the related and important finding that people who are more open to discrepant information make better predictions over the long run than those who are more strongly driven by powerful beliefs about how the world operates, see Tetlock, *Expert Political Judgment: How Good Is It? How Can We Know?* (Princeton, NJ: Princeton University Press, 2005).
9. Wesley K. Wark, *The Ultimate Enemy: British Intelligence and Nazi Germany* (Ithaca, NY: Cornell University Press, 1985); Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Ithaca, NY: Cornell University Press, 2011).

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. Instructors can access these resources at <http://college.cqpress.com/sites/intel-resources>.

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 H₂O,” “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.

1 Who Poisoned Karinna Moskalkenko?

Key Questions

- ▶ **Why is Karinna Moskalkenko a target?**
- ▶ **What tactics has Russia used in the past to poison opponents?**
- ▶ **Are there any common features among the alleged poisonings?**
- ▶ **Why do most observers believe that the Russian government is responsible for Moskalkenko's poisoning?**

CASE NARRATIVE

Karinna Moskalkenko is a prominent Russian human rights lawyer whose work in the Russian courts and at the European Court of Human Rights (ECHR) has gained her fame both at home and abroad. Her representation of prominent Kremlin foes in recent years has only heightened her profile; among these cases are her posthumous representation of Anna Politkovskaya, a Russian journalist widely known for her critical coverage of Moscow's policies toward Chechnya, and her representation of jailed former oil tycoon Mikhail Khodorkovsky. In 2008, Moskalkenko herself captured international headlines with news that she had fallen ill with mercury poisoning. Press reports indicated that she and her family—all of whom were living in Strasbourg, France, at the time of the incident in order to facilitate her work at the Strasbourg-based ECHR—were taken to a French hospital suffering from headaches, dizziness, and vomiting.¹ Moskalkenko told reporters that the poisoning may have been an attempt to frighten her before a pretrial date in the Politkovskaya case,² noting that “people do not put mercury in your car to improve your health.”³

Russia's Poisoned Past

Poison figures prominently in recent Russian politics. A rash of cases throughout the last decade in which Kremlin critics have suffered the effects of a range of toxins has added to an already long list of notable poisonings in Russian history (see Figure 1.1). While Russian government involvement in some of these recent cases has not been substantiated, allegations of Russian government-sponsored attacks against those who publicly criticize Moscow's policies have continued throughout the decade. The victims of the poisonings range widely from Russian journalists, lawyers, and businesspeople to foreign politicians and Chechen rebels.

Figure 1.1 ▶ Chronology of Alleged Russian Poisonings, 2000–2010

Year	Alleged Poisoning
2002	Omar Ibn al-Khattab, a Chechen Sunni jihadist, dies from a poisoned letter sent by the Russian FSB.
2003	Duma deputy and opposition newspaper editor Yuri Shchekochikin mysteriously dies. His family believes that he was a victim of poisoning—possibly with dioxin.
2004	Russian presidential candidate Ivan Rybkin goes missing for several days in advance of the election and later claims he was drugged by Russian authorities.
2004	Ukrainian presidential candidate Viktor Yushchenko is poisoned with dioxin; Yushchenko suspects a Ukrainian-Russian cabal.
2004	Russian journalist Anna Politkovskaya says she was poisoned on a flight she took to cover the Beslan school tragedy.
2006	Former KGB officer and later Kremlin critic Aleksander Litvinenko dies from polonium-210 radiation poisoning in London. The Russian government refuses Britain's request to extradite the prime suspect.

In some cases the targets have been longtime, self-declared foes of the Russian government who aim to destroy Russian interests just as much as Moscow aims to destroy the targets. Such was the case of Omar Ibn al-Khattab, a symbol of Islamic extremism and notorious guerrilla commander in the second Chechen war against Moscow. Khattab's guerilla roots can be traced back to the 1980s, when he fought against the Soviets in Afghanistan. He later participated in Muslim insurrections in the Soviet Central Asian republics. Khattab enlisted in the Chechen separatist movement in the mid-1990s and played a leading role in numerous attacks on Russian interests until his death in 2002. Press reports indicate that he was killed by a poisoned letter slipped to him by the Russian Federal Security Service (FSB), which had accused Khattab of links to al-Qaeda.⁴

Prominent Russian and foreign political leaders have also been targets of poisoning. In 2004, then-Russian presidential candidate Ivan Rybkin mysteriously disappeared for several days ahead of the election. When he resurfaced, he first told a garbled tale of travel to London and the Ukrainian capital, Kiev, but eventually he revealed that he had been drugged, abducted, and forced to make a compromising video by the FSB.⁵ He left politics after his ordeal. The fate of other Russian politicians has been far worse. Duma deputy Yuri Shchekochikin's family suspects that his puzzling death in 2003 was a result of poisoning by the toxin dioxin because he suffered an unexplained skin rash while investigating a company owned by high-level former KGB officials just before his death.⁶



Ukrainian presidential candidate Viktor Yushchenko experienced a rapid transformation in 2004 after ingesting the toxin dioxin. The photo on the left shows Yushchenko before being poisoned; on the right, after.

Also in 2004, then-Ukrainian presidential candidate Viktor Yushchenko underwent a dramatic transformation that medical experts determined was the result of dioxin poisoning. The Ukrainian prosecutor general said that tests confirmed Yushchenko suffered from poisoning by highly purified dioxin that is manufactured only in Russia, the United States, and Great Britain.⁷ Investigators received samples from all but Russia, which has kept “silent on the matter” despite two requests for a sample, according to the Ukrainian prosecutor general.⁸

The case remains unsolved, and as of August 2009, experts involved in Yushchenko’s treatment said that scientific analysis had not provided any more clues as to who was responsible for the poisoning.⁹ Nonetheless, many—including Yushchenko—speculate that the dioxin originated in Russia and was slipped to him during a dinner on 5 September 2004 with the head of the Ukrainian security services—which has close ties to Moscow—most likely in order to complicate Yushchenko’s bid for the presidency and to improve the chances of the Moscow-backed candidate Viktor Yanukovich.¹⁰ Russian officials have denied any Russian involvement in the case, saying, “There is no evidence to support such claims,” but former Soviet and Russian security services officers say that they believe the Russian security services may have been involved.¹¹

Reknowned Russian journalists such as Anna Politkovskaya have claimed to be targets of poisoning as well. Politkovskaya was born into the Soviet elite but committed herself to chronicling alleged Russian abuses in Chechnya. In a 2004 interview with the London-based *Guardian* newspaper, she said:

To this day there’s torture in any FSB branch in Chechnya, like the so-called “telephone,” where they pass an electric current through a person’s body. I’ve seen hundreds of people who’ve been through this torture. Some have been tortured in such an intricate way that it’s hard for me to believe that it was done by people who went to the same sort of schools that I did, who read the same textbooks.¹²

The same interview repeated her claims that that she nearly died in 2004 when she was slipped poison in a cup of tea while on her way to cover the Beslan school hostage tragedy. It also cited her claims of numerous death threats from Russian troops, noting that “the kidnappings, extrajudicial killings, disappearances, rapes and tortures she has reported on in Chechnya have left her convinced that Putin’s policies are engendering the terrorists they are supposed to eliminate.”¹³

Politkovskaya was gunned down in 2006 outside her apartment. The Russian government says that the murder was ordered from abroad by enemies of the state. Russian prosecutor general Yuri Chaika in 2007 said the killers hoped to “create a crisis situation and bring about a return to the old management system in which money and oligarchs decided everything.”¹⁴ Those who ordered the killing have not yet been identified.

Aleksander Litvinenko, a onetime Russian KGB officer whose public comments on KGB practices raised Moscow’s ire, himself fell ill after the radioactive isotope polonium-210 was slipped into his tea at an upscale London hotel in 2006.¹⁵ British officials traced a radioactive trail across London to Hamburg, Germany, and aboard British Airways planes that had flown to Moscow.¹⁶ The trail coincided with the routes of Andrei Lugovoi, a former KGB bodyguard whom British authorities have identified as the prime suspect, and his associate, Dmitri Kovtun.¹⁷ Litvinenko alleged on his deathbed that he had been poisoned at the behest of then-Russian president Vladimir Putin.¹⁸ The Russian government has denied British requests for extradition of Lugovoi, who claims that he is the scapegoat for a British intelligence plot executed with the help of self-exiled Russian tycoon Boris Berezovsky to create a political scandal.¹⁹ All involved deny the allegations.



Aleksander Litvinenko’s wife, Marina (third from left), announces the establishment of the Aleksander Litvinenko Foundation in 2007 with, from left, the family’s spokesperson Alex Goldfarb, human rights lawyer Louise Christian, and Russian billionaire Boris Berezovsky. Photos of Litvinenko before and after the poisoning appear above the presenters.

The Experts Concur

Although Russian officials either deny involvement in many of these cases or have simply ignored the allegations, several former KGB and FSB officers support the claims that Moscow

has used poisoning as a tool of intimidation, coercion, and murder.

In addition to Litvinenko, Oleg Gordievsky is another prominent former KGB colonel who has spoken out about Russia's tactics. Gordievsky, who defected to the United Kingdom in the mid-1980s, has lamented the "gangster mentality" that he says has spread through the FSB since 2000 and has accused Russia of becoming "a terrorist regime."²⁰ He has claimed "with certainty" that Politkovskaya's poisoning was the work of the FSB.²¹ The same is true, he says, of Shchekochikin and Litvinenko.

Oleg Kalugin, a former chief of KGB counterintelligence who defected to the United States, is also confident of the FSB's use of poison to silence its opponents. In a book he published in 1994, Kalugin detailed the KGB's use of a ricin-tipped umbrella to murder the Soviet dissident Sergei Markov.²² Litvinenko, he said in a 2006 interview, "fell victim to the Russian security services. They resort to murder, and poison is one of the weapons they have used for decades."²³ Vitaly Yurchenko, a KGB official who defected to the West in 1985, provides additional details to Kalugin's account of the KGB's role in Markov's murder, saying the KGB used "Special Lab 100" in Moscow to develop poisons for operational use, including the ricin used to kill Markov.²⁴

Moskalenko Falls Ill

It was against this backdrop that reports of Moskalenko's poisoning surfaced in October 2008 (see Figure 1.2). On Sunday, 12 October 2008, Moskalenko's husband discovered a dozen small pellets of mercury on the floor of the passenger and driver's side of their car as he, Moskalenko, and their three children arrived at church. Moskalenko's husband is a chemist and understood the pellets to be out of the ordinary. Moskalenko lodged a formal complaint with French authorities on 13 October. The French prosecutor's office deemed the discovery to be serious and opened an investigation.²⁵

Moskalenko and her family did not immediately note any symptoms at the time of their discovery of the mercury, but by Tuesday, 14 October, Moskalenko and her family complained publicly of nausea, headaches, and vomiting.²⁶ They were transported to a French hospital at the request of French officials for examination. By 16 October, press reports indicated that toxicology tests confirmed that the substance in the car was mercury.²⁷

The French Investigation

French officials did not immediately comment on the exact cause of the poisoning; neither did they explicitly rule in or out Russian involvement or any other cause. In public comments during the investigation, French authorities remained circumspect about both the physical effect that the amount of mercury found in the car could have on the family and the possible circumstances under which the mercury had found its way into the vehicle. The Strasbourg assistant prosecutor of the case, Claude Palpaceur, stressed that the quantity of mercury found was probably not sufficient to cause serious health consequences.²⁸ One French police official cited possible explanations for the mercury other than attempted poisoning, including that its presence could have been an accident or could have been associated with Moskalenko's purchase of the car in August 2008.²⁹

Figure 1.2 ▶ Chronology of the Karinna Moskalenko Poisoning

Date	Events
12 October 2008	Moskalenko's husband finds pellets of mercury in the family car.
13 October 2008	Moskalenko files a complaint with French authorities, who open an investigation.
14 October 2008	Moskalenko is taken to a French hospital with dizziness, headaches, and vomiting.
15 October 2008	Moskalenko misses a pretrial hearing in Moscow in the Anna Politkovskaya case.
16 October 2008	Press reports indicate that toxicology tests confirm mercury as the substance found in the Moskalenko vehicle.

Previous Pressure Tactics

This was not the first time that Moskalenko's struggles as a Russian human rights lawyer had captured headlines. Moskalenko also found herself in the spotlight in 2007, when the International Helsinki Foundation for Human Rights urged Russia to end its "ongoing harassment" against her, saying Moscow's efforts to disbar her "were aimed at punishing her for her work on politically sensitive cases."³⁰ Although Moskalenko's case record in Russian courts is full of numerous losses, she has won twenty-seven cases against Russia in the European Court of Human Rights and has more than one hundred other cases pending in the court that are an apparent thorn in Moscow's side.³¹

In addition to the personal pressure exerted on Moskalenko, in 2006, the International Protection Center, which she runs in Moscow, came under scrutiny by the Russian tax police. In response, Moskalenko opened a sister office in Strasbourg, France, to take up the slack should her Moscow office be closed by Russian authorities.³² In 2007, Moskalenko said that "across the whole world it is well known that lawyers who are carrying out their professional activities cannot be subjected to pressure.... But it seems to me that today's Russian authorities are not driven by logic."³³

International Press Coverage

News of Moskalenko's illness quickly hit the wires and was carried by prominent newspapers worldwide. The reports led with the familiar themes of Russian poisoning and political pressure, and in many cases they noted the curious timing of the poisoning, just a few days before the pretrial date in the Politkovskaya case:

French police fear that Russian agents may have tried to poison top human rights lawyer Karinna Moskalenko—a well-known critic of the Kremlin. They have started an inquiry after Ms. Moskalenko complained that "a substance similar to mercury" had been placed in her car in the French city of Strasbourg on Monday. "I feel worse and worse. My children also feel bad," she told reporters yesterday.... If confirmed as a poisoning, the Moskalenko case would carry echoes of the 2006 murder of former security service officer Litvinenko in London.

—*Courier Mail* (Australia)³⁴

A lawyer representing the family of investigative journalist Anna Politkovskaya has apparently been targeted by poisoners as the trial of three men accused of involvement in her murder was about to begin. French police confirmed the discovery of mercury pellets in the car of Karinna Moskalenko, who suffered headaches, dizziness and nausea after getting into the vehicle. Ms. Moskalenko was taken to hospital for tests in Strasbourg on Tuesday, which prevented her from flying to Moscow for the Politkovskaya trial.

—*Independent* (UK)³⁵

French Police are investigating how toxic mercury pellets ended up in the car of a human rights lawyer who fell ill in Strasbourg on Tuesday, a day before pretrial hearings in the Moscow into the killing of one of her best-known clients, the journalist and Kremlin critic Anna Politkovskaya.... Kremlin critics have often been the targets of poisoners. Ms. Politkovskaya herself fell ill after drinking a cup of tea while on her way to cover the aftermath of the Beslan school siege in which more than 300 people died.

—*International Herald Tribune*³⁶

Another lawyer for [jailed former Yukos oil executive] Khodorkovsky, Robert Amsterdam, said the timing was suspicious. “This type of event gives all pause to consider what it takes now in Russia to defend human rights. There are ongoing attacks on lawyers and journalists.... What matters is not if it’s related to Yukos or Politkovskaya but that it’s another human rights defender that’s in this situation.”³⁷

The Court of Public Opinion

Within days of the Moskalenko poisoning, the international court of public opinion, including newspapers, journals, blogs, television, and radio, was looking askance at Russia. The *Washington Post* editorial page, on 22 October 2008, stated the verdict most plainly:

Perhaps this was an unfortunate accident; the police in Strasbourg say they are still investigating. But history suggests otherwise. Numerous opponents of Mr. Putin have been killed or gravely sickened by poisoning. They include Ukrainian President Viktor Yushchenko; dissident former KGB officer Litvinenko; journalist Yuri Shchekochikin; and Ms. Politkovskaya.³⁸

RECOMMENDED READING

Andrew, Christopher, and Vasili Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books, 1999.

Table 1.1 ▶ 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

WHO POISONED KARINNA MOSKALENKO?

Structured Analytic Techniques in Action

Analysts often are asked to render judgments on fast-breaking events for which there is limited information. In these situations, the Premortem Analysis, Structured Self-Critique, and Starbursting can help analysts avoid a rush to judgment and illuminate important areas for further consideration by facilitating creative thinking and simply asking the right questions.

Technique 1: The Premortem Analysis and Structured Self-Critique

The goal of these techniques³⁹ 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.

Task 1. Conduct a Premortem Analysis and Structured Self-Critique 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.

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

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 much would this affect the analysis?

STEP 5: Is there any contradictory or anomalous information? Was any information overlooked

that is inconsistent with the lead hypothesis?

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

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

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 1.2.)

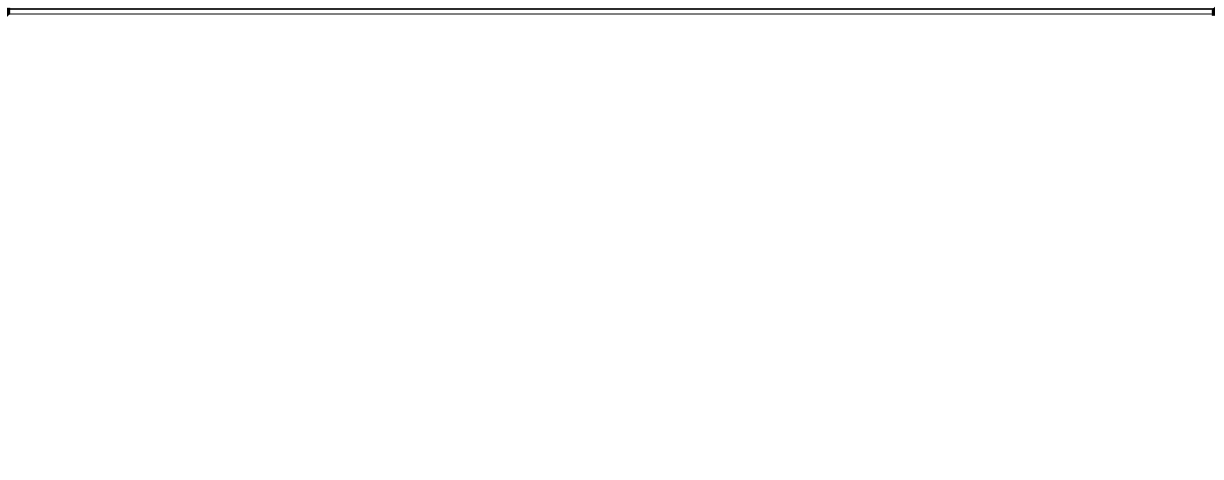
STEP 9: Based on the answers to the themes of inquiry outlined, list the potential deficiencies in the argument in order of potential impact on the analysis.

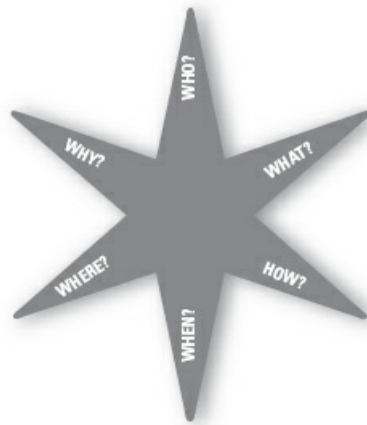
Analytic Value Added. As a result of your analysis, would you retain, add a caveat to, or dismiss the mainline judgment, and why?

Table 1.2 ▶ 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.

Figure 1.3 ▶ Starbursting Template





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.

Technique 2: 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.

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?*
- 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.
- 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 deserve further investigation?

NOTES

1. Miriam Elder, “Poison Stalks Trial of Murdered Putin Critic,” *Independent* (London), October 16, 2008, <http://www.independent.co.uk/news/world/europe/poison-stalks-trial-of-murdered-putin-critic-962727.html>.
2. Steve Gutterman, “Anti-Kremlin Lawyer Fears Mercury Poisoning Plot,” *Advertiser* (Adelaide, Australia), October 17, 2008.
3. Michael Schwartz and Alan Cowell, “Toxins Found in Russian Rights Lawyer’s Car,” *International Herald Tribune*, October 15, 2008, <http://www.nytimes.com/2008/10/16/world/europe/16russia.html>.

4. "Obituary: Chechen Rebel Khattab," *BBC News*, April 26, 2002, <http://news.bbc.co.uk/2/hi/europe/1952053.stm>.
5. Scott Peterson and Fred Weir, "KGB Legacy of Poison Politics," *Christian Science Monitor*, December 13, 2004, <http://www.csmonitor.com/2004/1213/p01s02-woeu.html>.
6. Ibid.
7. "Russia 'Silent' on Poison Inquiry," *BBC News*, July 6, 2007, <http://news.bbc.co.uk/2/hi/europe/6278524.stm>.
8. Ibid.
9. Associated Press, "Yushchenko Poison Made in Lab, Study Says," *Boston.com*, August 5, 2009, http://articles.boston.com/2009-08-05/news/29266668_1_dioxin-levels-poison-ukrainian-presidential-candidate/.
10. Scott Shane, "Poison's Use as Political Tool: Ukraine Is Not Exceptional," *New York Times*, December 14, 2004, <http://www.nytimes.com/2004/12/15/international/europe/15poison.html>; Tony Halpin, "Viktor Yushchenko Points Finger at Russia over Poison That Scarred Him," *Times* (London), September 11, 2007, <http://www.timesonline.co.uk/tol/news/world/europe/article2426190.ece>; Ron Synovitz, "Ukraine: Yushchenko Convinced He Was Poisoned by 'Those in Power,'" "Radio Free Europe/Radio Liberty, December 13, 2004, <http://www.rferl.org/content/article/1056378.html>.
11. Shane, "Poison's Use as Political Tool."
12. James Meek, "Dispatches from a Savage War," *Guardian*, October 15, 2004, <http://www.guardian.co.uk/world/2004/oct/15/gender.uk>.
13. Ibid.
14. "Anna Politkovskaya," *New York Times*, updated June 26, 2009, http://topics.nytimes.com/topics/reference/timestopics/people/p/anna_politkovskaya/index.html.
15. This bizarre poisoning by a radioactive substance is not the first reported incident of such tradecraft. Indeed, a postmortem investigation into the death of a former Putin bodyguard, Roman Tsepov, two years before the Litvinenko poisoning in 2004 found that Tsepov had been poisoned by an unspecified radioactive material. See Jonathan Calvert, "The Putin Bodyguard Riddle," *Sunday Times* (London), December 3, 2006, <http://www.timesonline.co.uk/tol/news/uk/article658488.ece>. Tsepov had survived three previous assassination attempts in the 1990s. See "King of Shadows Poisoned," *St. Petersburg Times* (Russia), September 28, 2004, http://www.sptimes.ru/index.php?action_id=2&story_id=1697.
16. Jon Elsen, "Alexander V. Litvinenko," *New York Times*, May 31, 2007, http://topics.nytimes.com/topics/reference/timestopics/people/l/alexander_v_litvinenko/index.html.
17. Ibid.
18. Ibid.
19. Ibid.
20. Oleg Gordievsky, "Russia's Killing Ways," *Washington Post*, December 14, 2006, <http://www.washingtonpost.com/wp-dyn/content/article/2006/12/13/AR2006121301909.html>.
21. Ibid.
22. David Wise, "Poison with a Familiar Scent," *Los Angeles Times*, November 26, 2006, <http://articles.latimes.com/2006/nov/26/opinion/op-wise26>.
23. Ibid.
24. Ibid.
25. Cyrille Louise and Laure Mendeveille, "Une avocate russe affirme avoir été empoisonnée [Russian lawyer shown to have been poisoned]," *Le Figaro* (France), October 14, 2008, <http://www.lefigaro.fr/actualite-france/2008/10/15/01016-20081015ARTFIG00023-une-avocate-russe-affirme-avoir-ete-empoisonnee-.php>.
26. Ibid.
27. Ibid.
28. Ibid.
29. Ibid.
30. "Russia Urged to End Harassment against Lawyer," Radio Free Europe/Radio Liberty, May 9, 2007, <http://www.rferl.org/content/article/1076361.html>.
31. Yuri Zarakhovich, "Murder, Russian-Style: Political Assassination," *Time*, October 19, 2008, <http://www.time.com/time/world/article/0,8599,1851854,00.html>.
32. Peter Finn, "Russia's Champion of Hopeless Cases Is Targeted for Disbarment," *Washington Post*, June 3, 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/06/02/AR2007060201135.html>.
33. Christian Lowe, "Russian Defense Lawyers in Hazardous Profession," Reuters, July 23, 2007, <http://www.reuters.com/article/2007/07/23/us-russia-justice-lawyers-idUSL2171073820070723>.
34. "Kremlin Foe 'Poisoned' Lawyer Says: Mercury Placed in Her Vehicle," *Courier Mail* (Brisbane, Australia), October 16, 2008, <http://www.nexislexis.com/>.
35. Elder, "Poison Stalks Trial of Murdered Putin Critic."
36. Schwirtz and Cowell, "Toxins Found in Russian Rights Lawyer's Car."

37. Elder, "Poison Stalks Trial of Murdered Putin Critic."
38. "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>.
39. 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).

2 The Anthrax Killer

Key Questions

- ▶ Who is the main person of interest in the case, and why?
- ▶ What is the evidence in the case?
- ▶ What are the strengths and weaknesses of the government's case?

CASE NARRATIVE

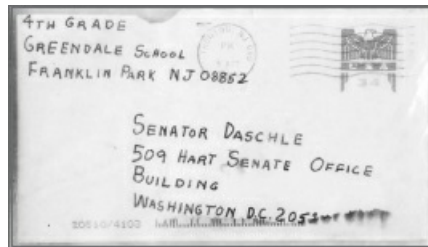
It Looked Like Baby Powder

On 15 October 2001, Sen. Tom Daschle's office in the Hart Senate Office Building in Washington, D.C., was teeming with staffers, interns, and volunteers like Bret Wincup. He and an intern, Grant Leslie, were opening the piles of letters Senator Daschle received on a daily basis. As Leslie opened a letter, a fine white substance that looked like baby powder landed on the desk, her skirt, and shoes. "We both kind of commented on it," said Wincup, but initially no one knew how alarmed to be.¹ Usually, these types of scares were hoaxes. But this time, it was no hoax. Within an hour, Navy infectious disease specialist Greg Martin had arrived at Senator Daschle's office to investigate, and by the end of the day the white powder was confirmed as a deadly dose of anthrax. For Wincup, it was the point at which "people with white suits came in.... That was scary."² He would later discover just how great a threat that powder represented: opening a letter laced with that number of anthrax spores could result in an exposure that was one thousand to three thousand times the lethal dose,³ and anyone who came into contact with these spores was at risk for developing this highly virulent infectious disease. Emergency personnel quickly quarantined the Hart Office Building, and staffers began treatments with the potent antibiotic Cipro. The incident riveted the attention of the nation: Who could be behind the attack, and how far might it spread?

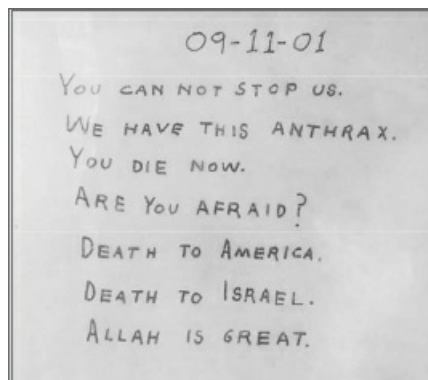
A Nation under Siege

When Grant Leslie opened the letter, the United States was still reeling from the terrorist attacks of 9/11 that had taken nearly three thousand lives only a month before. By October, Capitol Hill was just returning to normal operations, and the United States was gearing up for war against terrorists hiding in Afghanistan. The attacks on 9/11 had already prompted a bioterrorism scare, including a run on antibiotics in New York City and elsewhere.⁴ Reports that the United States was low on supplies of anthrax vaccine only fueled fears.⁵ The government urged against hoarding of the only Food and Drug Administration (FDA)-approved antibiotic used to treat

anthrax, Cipro, while infectious disease specialists cautioned that Cipro had never been tested in a clinical setting, making it unclear if the drug would be effective in the event of a real anthrax attack.⁶



Envelope sent to Senator Daschle's office.



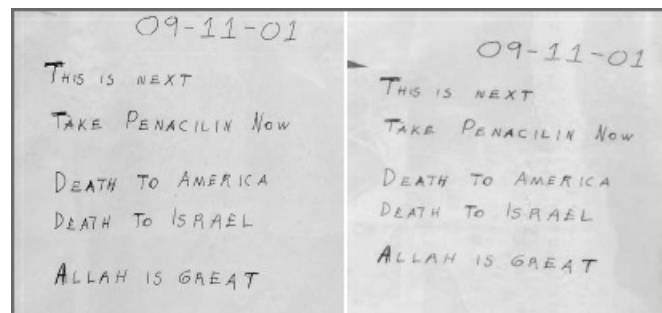
Letter sent to Senator Daschle's office.

Fears about anthrax had swirled in Florida and in the national headlines since early October. Reports that Robert Stevens, a sixty-two-year-old photo editor who worked in Boca Raton, was hospitalized with inhalation anthrax on 2 October and died on 5 October, prompted Secretary of Health and Human Services Tommy Thompson to note in a White House briefing that the case was isolated and not contagious, adding, "There is no terrorism."⁷ Nevertheless, both the Centers for Disease Control (CDC) and the Federal Bureau of Investigation (FBI) were actively investigating the unusual case when Ernesto Blanco, Stevens's coworker at the American Media, Inc., building in Boca Raton, was diagnosed with inhalation anthrax on 5 October. Stevens had fallen ill and sought medical treatment on 2 October after handling a letter laced with a fine "white talc" on 19 September, and Blanco had fallen ill and sought medical treatment on 1 October.⁸ Blanco's treatment was successful, and he was discharged on 17 October. In response to Blanco's diagnosis, the FBI began a criminal investigation into the Florida anthrax cases on 8 October. As forty FBI agents descended on the American Media building, which was home to the *Sun* and several other tabloids, including the *National Inquirer*, Attorney General John Ashcroft said that although "we are taking the matter very seriously ... we don't know enough to know if this is related to terrorism or not."⁹ Authorities would soon get the information they needed.

In New York, news reports surfaced on 13 October about another anthrax case. On 25 September, Erin O'Connor, an assistant to NBC correspondent Tom Brokaw, handled a

threatening letter that was postmarked 18 September in Trenton, New Jersey. She developed cutaneous anthrax and sought medical attention on 1 October.¹⁰ On 28 September, Casey Chamberlain, another assistant to Tom Brokaw who had originally opened the letter, also developed cutaneous anthrax.¹¹ The O'Connor and Chamberlain cases were followed by reports on 20 October of a *New York Post* employee, Johanna Huden, who also had cutaneous anthrax. She noticed a bump on her finger on 21 September and spent weeks seeing numerous physicians before she self-diagnosed the problem after reading news reports about the cases in Florida and New York. Her colleagues, an unnamed *New York Post* mailroom employee and editor Mark Cunningham, also developed cutaneous anthrax on 19 and 23 October, respectively. Cunningham noticed symptoms after going through old mail, some of which was postmarked in September.¹² And in a disturbing development at the ABC offices in New York, the seven-month-old son of an ABC employee developed cutaneous anthrax on 29 September after visiting his mother's office and was admitted to the hospital on 1 October.¹³ Also on 1 October, Claire Fletcher, an assistant to *CBS News* anchor Dan Rather, developed cutaneous anthrax. She recovered quickly, no one else in the *ABC News* office fell ill, and there was no envelope or other source of the bacteria to account for Fletcher's illness, prompting Rather to say that "our biggest problem is not anthrax.... Our biggest problem is fear."¹⁴

As the New York reports came in, copycat cases raised investigators' ire. Three St. Petersburg, Florida—postmarked letters arrived at media outlets in New York containing a powder that tested negative for anthrax muddied the waters and were described as a "tremendous drain on resources" by the New York FBI office.¹⁵ Attorney General Ashcroft said the FBI was dealing with dozens of anthrax hoaxes, and warned that the Justice Department would vigorously prosecute those involved in hoaxes, which would be prosecuted as federal felonies.¹⁶



Letters sent to *NBC News* anchor Tom Brokaw (left) and the *New York Post* editor (right).

Cases also began to surface among postal workers at the Hamilton Township mail center in New Jersey, but unlike in New York, they were a mix of both cutaneous and inhalation anthrax. Victims included Richard Morgano, who presented with cutaneous anthrax on 26 September after scratching his arm on the job while fixing a jammed machine on 18 September.¹⁷ His colleague, mail carrier Teresa Heller, fell ill with cutaneous anthrax on 28 September. Another colleague, Norma Wallace, was diagnosed on 19 October with inhalation anthrax after a colleague shot compressed air into a jammed machine that sent dust particles into the air on 9 October.¹⁸ Patrick O'Donnell, another Hamilton postal worker, developed symptoms on 14 October. This time, it was an acute case of cutaneous anthrax that kept him in the hospital for a week.¹⁹ The next day, Jyotsna Patel, also a postal worker, developed inhalation anthrax and

spent the eight days in the hospital, while Linda Burch, an accountant at the same facility, developed a lesion on her forehead on 17 October.²⁰

The picture in Washington, D.C., quickly darkened. The anthrax letter that arrived at Senator Dashle's office on 15 October shut down Congress for the second time in two months.²¹ In addition to Leslie and Wincup, twenty-nine others on the Hill tested positive for exposure but did not develop anthrax symptoms. At the Brentwood mail facility, which processes mail bound for Capitol Hill, postal workers quickly succumbed to the disease. Leroy Richmond, an anonymous patient dubbed "George Fairfax," Thomas Morris Jr., and Joseph Curseen Jr. developed inhalation anthrax on 16 October.²² Richmond and the anonymous patient survived, and Morris and Curseen succumbed to their illnesses on 21 and 22 October, respectively. Nearby, a postal worker at the State Department mail center in Sterling, Virginia, named David Hose developed inhalation anthrax on 22 October but survived.²³

Two fatal inhalation anthrax cases in New York and Connecticut proved to be the most baffling. In New York, a stockroom attendant at Manhattan Eye, Ear and Throat Hospital named Kathy Nguyen became ill on 25 October and died on 31 October.²⁴ In nearby Connecticut, a ninety-four-year-old woman named Otilie Lundgren became ill on 14 November and died on 21 November in a hospital in Derby, Connecticut. Like the *ABC News* office case, there was no known source of exposure, and therefore no immediate explanation for the women's deaths.²⁵

By mid-November, authorities faced a total of twenty-two confirmed cases of anthrax, thirty-one positive cases of exposure, and another ten thousand cases deemed "at risk" from exposure.²⁶ Eleven of the twenty-two victims suffered from cutaneous anthrax but recovered after long courses of antibiotics. The remaining eleven suffered from the more deadly form of inhalation anthrax; only six survived.

The Amerithrax Task Force

In response to Robert Stevens's death and the letters found in New York and Washington, D.C., the FBI opened one of the largest investigations in its history—Amerithrax. Given the geographic scope of the investigation, FBI field offices in Miami, New York, New Haven, Baltimore, and Washington, D.C.—designated the lead office—participated. Nearly thirty full-time investigators from the FBI, US Postal Inspection Service, and the US Attorney's Office for the District of Columbia formed the core of the task force.²⁷

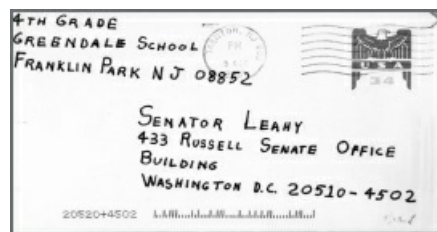


Envelopes sent to *NBC News* anchor Tom Brokaw (left) and *the New York Post* editor (right).

Initially, the Amerithrax task force did not know whether the letters were an act of a state-sponsored terrorist group, an international terrorist organization, a domestic terrorist group, or an individual.²⁸ Investigators cast a broad net and scrutinized more than a thousand potential

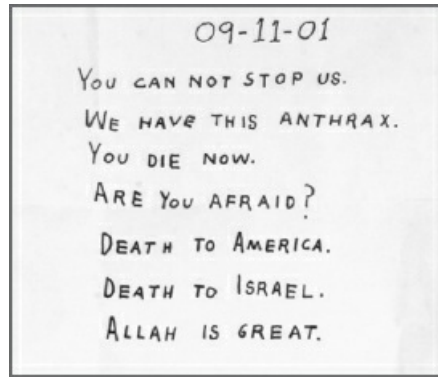
suspects in the United States and abroad.²⁹ This led to in-depth investigations of three hundred individuals, in addition to extensive scientific investigation of the letters, buildings, victims, and other physical objects connected to the case.³⁰

On 15 November, investigators received another piece of evidence. While searching through quarantined Capitol Hill-bound mail, FBI and Environmental Protection Agency agents found a letter addressed to Sen. Patrick Leahy that tested positive for anthrax. The letter had found its way into the quarantined mail after an optical scanner misread the zip code on the letter and sent it to the State Department mail facility rather than to the Capitol. It was then rerouted to the Hill, but it did not get there before the mail system shut down and the mail was quarantined.³¹ This brought the total number of anthrax letters to four: two sent to New York addresses at the *New York Post* and the *NBC News* office of Tom Brokaw, and two sent to the Capitol Hill offices of Senators Daschle and Leahy. All four letters bore a Trenton, New Jersey, postmark, although the New York envelopes were dated 18 September and the Washington-bound envelopes were dated 9 October. In addition, the New York envelopes had no return address, while the Washington-bound envelopes bore a fictitious New Jersey return address at the “Greendale School.” Investigators did not find a letter in Florida, but environmental testing of the American Media building found it to be a hot zone for anthrax, especially in Stevens’s office space.



The envelope sent to Senator Leahy and found by investigators on November 15, 2001, bore striking resemblance to the previous envelopes.

Given the scientific challenges presented by a bioterrorism attack using anthrax, the FBI received assistance from “29 government, university and commercial laboratories, which augmented FBI Laboratory efforts to develop the physical, chemical, genetic, and forensic profiles of the anthrax spore, letters, and envelopes used in the attacks.”³² By 18 October, the Centers for Disease Control confirmed that the strains of anthrax in the Daschle and Brokaw letters matched, as did the handwriting and written threats.³³ The spores in the New York letters also were found to match each other.³⁴ Also in October, Northern Arizona University microbiologist Paul Keim pinpointed the strain of anthrax used in the letter: it was a strain called the Ames strain that was derived from a cow in Sarita, Texas, in 1981.³⁵ Keim called the find “chilling” because the Ames strain was developed in US government laboratories.³⁶ In an independent test, the CDC came to the same conclusion. It was the Ames strain. In June 2002, the FBI announced that radiocarbon dating indicated that all the spores had been created within two years of the attack.³⁷



The letter sent to Senator Leahy was identical in text to the letter sent to Senator Daschle.

It took nearly a year for the task force to track down the mailbox from which the letters were mailed. Although the letters all bore the Trenton, New Jersey, postmark, that facility served 48 post offices and 625 of the ubiquitous blue street-side mailboxes. Theoretically, all of them would have to be tested. On the 621st try in August 2002, they found a mailbox in Princeton, New Jersey, that was heavily contaminated with anthrax.³⁸

Investigators and scientists eventually developed a profile of a likely suspect that included scientific ability, laboratory access to the Ames strain of anthrax, proximity and other links to New Jersey, and suspicious behavior. In late June, officials acknowledged that they had no prime suspect and that they maintained a list of fifty possible individuals.³⁹ By July 2002, a profile was featured in the media that described the suspect as “a loner, a science nerd with access to a sophisticated lab. He has a reason to be peeved, and he’s familiar with the Trenton, N.J. area. This Unabomber-like person, officials say, mailed the anthrax-laced letters last fall that resulted in five deaths.”⁴⁰

COPY

Analysis of Sample

Date analyzed - 17 October, 2001
Date of Report - 18 October, 2001

Sample SPC-257, letter/powder

I received the sample (in ziplock bags) from [redacted] on the afternoon of 17 October, 2001. The sample was taken into B-3. Insufficient powder was on the letter, so powdery material was scraped from the envelope and put into a small, tared, glass container. The container was reweighed and the net weight of the powdery material was determined to be 0.013 grams. To the material was added 987 μ l of sterile water for injection to make a total of 1 gram (and approximately 1 ml) of suspension. Ten-fold dilutions were plated out onto TSA, then incubated overnight. Plate counts were made, and it was determined that the original tube contained 2.72×10^{10} CFU per ml. Since there was 0.013 grams of material, this calculates to be 2.1×10^{12} CFU per gram of powder material.

Visual inspection of the suspension of material under phase contrast microscopy found no visible vegetative cells, no visible debris, and very few small clumps. Most of the material appeared to be individual refractile spores.

Interpretations and conclusions: If this is a preparation of bacterial spores, it is an extremely pure preparation, and an extremely high concentration. These are not "garage" spores. The nature of the spore preparation suggests very highly that professional manufacturing techniques were used in the production and purification of the spores, as well as in converting the spores into an extremely fine powder.

Bruce E. Ivins, 18 Oct. 2001

Bruce E. Ivins, Ph.D.
USAMRIID Bacteriology Division

An assessment by an anthrax specialist at the US Army Medical Research Institute of Infectious Disease at Ft. Detrick, Maryland, found the spores to be extremely fine, requiring professional manufacturing techniques.

Box 2.1 FBI Linguistic and Behavioral Assessment

In a 9 November 2001 press briefing, the FBI released a linguistic and behavioral assessment of the letters that had been received to date. In addition to noting that "it is highly probable, bordering on certainty, that all three letters were authored by the same person," the FBI offered the following behavioral assessment and requested the public's help to identify the killer.

Based on the selection of Anthrax as the "weapon" of choice by this individual, the offender:

- ▶ is likely an adult male.
- ▶ if employed, is likely to be in a position requiring little contact with the public, or other employees. He may work in a laboratory. He is apparently comfortable working with an extremely hazardous material. He probably has a scientific background to some extent, or at least a strong interest in science.
- ▶ has likely taken appropriate protective steps to ensure his own safety, which may include the use of an Anthrax vaccination or antibiotics.

- ▶ has access to a source of Anthrax and possesses knowledge and expertise to refine it.
- ▶ possesses or has access to some laboratory equipment; i.e., microscope, glassware, centrifuge, etc.
- ▶ has exhibited an organized, rational thought process in furtherance of his criminal behavior.
- ▶ has a familiarity, direct or indirect, with the Trenton, NJ, metropolitan area; however, this does not necessarily mean he currently lives in the Trenton, NJ, area. He is comfortable traveling in and around this locale.
- ▶ did not select victims randomly. He made an effort to identify the correct address, including zip code, of each victim and used sufficient postage to ensure proper delivery of the letters. The offender deliberately “selected” NBC News, the *New York Post*, and the office of Senator Tom Daschle as the targeted victims (and possibly AMI in Florida). These targets are probably very important to the offender. They may have been the focus of previous expressions of contempt which may have been communicated to others, or observed by others.
- ▶ is a non-confrontational person, at least in his public life. He lacks the personal skills necessary to confront others. He chooses to confront his problems “long distance” and not face-to-face. He may hold grudges for a long time, vowing that he will get even with “them” one day. There are probably other, earlier examples of this type of behavior. While these earlier incidents were not actual Anthrax mailings, he may have chosen to anonymously harass other individuals or entities that he perceived as having wronged him. He may also have chosen to utilize the mail on those occasions.
- ▶ prefers being by himself more often than not. If he is involved in a personal relationship it will likely be of a self serving nature.

Source: Amerithrax Press Briefing, “Linguistic/Behavioral Analysis of the Anthrax Letters,” Federal Bureau of Investigation, November 9, 2001, <http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax/linguistic-behavioral-analysis-of-the-anthrax-letters>.

An Inside Job?

Once investigators learned that the anthrax used in the attacks was the Ames strain, they were able to focus their efforts on places where it was researched and stored. Using this information and the profile, investigators by late July 2002 had narrowed their search to thirty people at two US government installations: the US Army Medical Research Institute of Infectious Disease (USAMRIID) at Ft. Detrick, Maryland, and Dugway Proving Ground in western Utah.⁴¹ Both of these facilities began as military sites associated with the erstwhile US offensive biological weapons program. When President Richard Nixon disbanded the offensive program in 1969, he ordered that future work be confined to “research in biological defense, on techniques of immunization, and on measures on controlling and preventing the spread of disease.”⁴²

In 2001, scientists at these facilities were focusing their efforts on just this kind of defensive

research. They retained small stocks of deadly viruses and bacteria in order to study them and create better vaccines. They also served as the nation's repository of expertise in anthrax. In a bizarre catch-22, investigators interviewed these scientists, sometimes repeatedly, as potential suspects, while at the same time relying on many of these same scientists to use their unique skills to test the thousands of samples involved in the case. According to one scientist at USAMRIID, where the Ames strain was developed and researched, "Between 11 Sept. and May, USAMRIID processed over 31,000 samples and 260,000 assays in our forensic-based lab." They usually processed just four to six samples a month.⁴³ During this period, scientists often worked hundred-hour weeks, and many slept in their labs or cars.

Even as the scientists did this sensitive work, questions about the safety and security of both facilities arose. USAMRIID was specially equipped to handle this kind of work and appeared to take appropriate measures to ensure the safety and security of the labs, according to a July 2002 press report:

The labs where USAMARIID does this very dangerous work are reached from the office suites through a long, tan wallpapered hall and a metal door that opens only after a worker scans a magnetic identification card. Ahead are labyrinthine halls and labs—50,000 square feet at biosafety level 3, where agents like anthrax, plague, and Venezuelan equine encephalitis are studied, and the 10,000 square feet at biosafety level 4, where research is done with the most deadly agents, like Ebola and Marburg. To get into any of those, the worker needs to re-enter the magnetic card, along with a four-digit number that's only issued after the worker has been immunized against that particular bug. The doors are also keyed in to central security, so there is a master list of who enters and exits the labs.⁴⁴

Reports about security at Dugway Proving Ground, however, were less glowing. One former scientist at Dugway who directed biological safety from 1989 to 1993 publicly accused the facility of "sloppy handling" of anthrax spores.⁴⁵ He cited anthrax spores stored in unsecured refrigerators in hallways, plans for production of thirty gallons of wet anthrax, and poor lab safety procedures. Officials at the base, however, refuted the claims.⁴⁶

As their work progressed, investigators narrowed their focus on these same scientists who were aiding the investigation. On the basis of a tip, agents drained a pond near USAMRIID in June 2002 in Frederick, Maryland, in search of anthrax evidence. None was found. They searched the homes of scientists but named no suspects. By the end of July investigators had "interviewed some 5,000 people, issued 1,700 grand jury subpoenas, polygraphed hundreds of people, and created 112 databases just for this case."⁴⁷ Some scientists who had been interviewed told the press that "the FBI's line of questioning in interviews with microbiologists suggested that the Bureau believed the anthrax spores could have been grown in secret inside Fort Detrick."⁴⁸

Despite the FBI's efforts, by August 2002 there were still no suspects. With the one-year anniversary of the first two letters looming, pressure was building for the task force to name a suspect. A *New York Times* editorial called the FBI investigation "unbelievably lethargic." Unnamed government officials raised the specter of more attacks in the context of the FBI's slow investigation, telling the British newspaper the *Guardian* that "it was grown, and therefore it can be grown again and again."⁴⁹

On 6 August 2002, the government publicly announced that it had a person of interest in the

case. In an unprecedented move, Attorney General John Ashcroft announced on the CBS *Early Show* that investigators had identified Steven J. Hatfill as a person of interest.⁵⁰

A Person of Interest

After nearly a year-long investigation, the announcement of a single person of interest caused both alarm and relief. Investigators trained their eyes on Hatfill because of his prior work at USAMRIID and tips from other scientists. Hatfill's background, scientific capabilities, and activities around the time of the anthrax letters contributed to the FBI's increased scrutiny of him and ultimately its public announcement of him as a person of interest in the case.

Steven J. Hatfill's background was indeed interesting to investigators. An extroverted ex-military member, he had spent most of his adult life living in Africa in the midst of wars and epidemics, worlds removed from his upbringing in Illinois, where he was born in 1953. He attended Southwestern University to study biology but left his studies for the Democratic Republic of Congo, where he worked at a Methodist mission hospital. While there, he honed his biology skills working in the lab. When he returned to the United States, he finished college and joined the Army, but he left when his poor vision prevented him from becoming a pilot. He subsequently returned to Africa, where he lived from 1978 to 1994 and later claimed to have completed a medical degree in Zimbabwe (then Rhodesia) near a suburb called Greendale. Investigators later discovered that Hatfill had allegedly forged his doctorate, a claim his lawyer publicly confirmed.⁵¹ During the time he lived in Africa, there were frequent outbreaks of anthrax in livestock—a common occurrence in a civil war-racked region, when animals went unvaccinated. Hatfill made good use of his US Army background during this time by serving as a volunteer Rhodesian Army medic during the civil war. After returning from Africa, he completed a postdoctoral degree and received three master's degrees before accepting a fellowship at Oxford. As a virologist, he returned to the United States to work on Ebola and other viruses at the National Institutes of Health (NIH) in Bethesda, Maryland.⁵² From there, he got a job at USAMRIID.

Investigators first interviewed Hatfill in early 2002. Other scientists and analysts had been urging them to look more closely at Hatfill because of his background in Africa, scientific capabilities, and activities around the time of the anthrax attacks.⁵³ Investigators specifically noted that Hatfill had worked at USAMRIID from 1997 until 1999, and according to the FBI, had “virtually unrestricted access to the Ames strain of anthrax” during that time.⁵⁴ Also, like many in the biodefense community who developed training scenarios, Hatfill understood how to disseminate anthrax through the mail.⁵⁵ In fact, he had given an interview while he was still at NIH about how to weaponize bubonic plague using only simple equipment.⁵⁶ He had also shown his ingenuity and expertise in other ways: he oversaw the construction of a full-scale model of an Iraq mobile biological weapons lab and taught the military how to destroy it, in addition to helping to prepare a 1999 brochure for emergency personnel on how to handle anthrax hoaxes.⁵⁷ His unpublished book about a bioterrorism attack on Washington, D.C. also raised suspicion, as did his work in Rhodesia during a large anthrax outbreak in the late 1970s. Last, he had filled multiple prescriptions for Cipro in 2001 and was taking the drug in September when two of the anthrax letters had been postmarked.⁵⁸

Investigators first searched Hatfill's apartment and his rented storage unit in Florida with Hatfill's consent on 25 June 2002. They returned on 1 August to search the apartment again. This time, using a search warrant, they searched not only his apartment, but also the trash bins outside

his building, coming up empty. Press reports at the time stressed that he had not been accused of any wrongdoing, but he “is the only person known to have been subjected to such intensive scrutiny.”⁵⁹ Following Attorney General Ashcroft’s 6 August announcement that Hatfill was a person of interest in the case, the FBI searched Hatfill’s apartment again on 11 August. All the while, Hatfill asserted his innocence. On 12 August, Hatfill held his own press conference outside his attorney’s office, saying:

I am appalled at the anthrax terrorist incident, and I wish the authorities Godspeed in catching the culprits or culprit. I do not object to being considered a subject of interest by the authorities because of my knowledge and background in the field of biological warfare defense. But I do object to an investigation characterized, as this one has been, by outrageous official statements, calculated leaks to the media and causing a feeding frenzy operating to my great prejudice. I especially object to having my character assassinated by reference to events from my past.... I know nothing about this matter.⁶⁰

Investigators had reasons to think differently. In their eyes, Hatfill’s background, travel, scientific capabilities, and access most certainly made him a person of interest, if not yet a prime suspect in the case.

RECOMMENDED READING

Amerithrax Investigation Summary. *Department of Justice*. Washington, DC: Department of Justice. February 19, 2010. <http://www.justice.gov/amerithrax>.

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

THE ANTHRAX KILLER

Structured Analytic Techniques in Action

Analysts are often called upon to support government task force investigations in which the fast pace of events, high level of scrutiny, and sheer quantity of information can be overwhelming. In the face of this kind of challenge, Chronologies, Timelines, Maps, and the Premortem Analysis and Structured Self-Critique can become essential tools for tracking, evaluating, sharing, and troubleshooting a large amount of data. In this case, Steven Hatfill was identified as the FBI's main person of interest. In the following exercises, students put themselves in the shoes of FBI analysts who must unravel how events in the case unfolded, present the information to a senior policy maker in a succinct format, and analyze the evidence prior to a decision on identifying persons of interest.

Techniques 1, 2, and 3: Chronology, Timeline, and Map

Chronologies are simple but useful tools that help 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 a 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.

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 the events occurred. Consider how best to array the data along the Timeline. Can any of the information be categorized?

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 such that it could be used as a graphic for a briefing with a high-level official.

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.

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?

Technique 4: The 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.⁶¹

Task 1. Conduct a Premortem Analysis 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 suddenly learn from an unimpeachable source that the judgment was wrong. Then imagine what could have caused the analysis to be wrong.

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

- STEP 2:** Use a brainstorming technique to identify alternative hypotheses for how the poisoning could have occurred. Keep track of these hypotheses.
- 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?
- STEP 5:** Is there any contradictory or anomalous information? Was any information overlooked that is inconsistent with the lead hypothesis?
- STEP 6:** Is there a potential for deception? Does anyone have motive, opportunity, and means to deceive you?
- STEP 7:** Is there an absence of evidence, and does it influence the key judgment?
- STEP 8:** Have you considered the presence of common analytic pitfalls such as analytic mindsets, confirmation bias, “satisficing,” premature closure, anchoring, and historical analogy?
- 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.

Analytic Value Added. As a result of your analysis, what are the strengths and weaknesses 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?

NOTES

1. Emily Pierce, "Anthrax Attack Victims Break Their Silence," *Roll Call News*, October 13, 2011, http://www.rollcall.com/issues/57_41.
2. Ibid.
3. Ibid.
4. Tamar Lewin, "A Nation Challenged: Fear of Infections; Anthrax Scare Prompts Run on an Antibiotic," *New York Times*, September 27, 2001, <http://www.lexisnexis.com.ezproxy.umuc.edu/hottopics/lnacademic>.
5. "U.S. Short of Vaccine for Deadly Anthrax," *Toronto Star*, September 20, 2001, <http://www.lexisnexis.com.ezproxy.umuc.edu/hottopics/lnacademic>.
6. Lewin, "A Nation Challenged."
7. Gina Kolata, "Florida Man Is Hospitalized with Pulmonary Anthrax," *New York Times*, October 5, 2001, <http://www.lexisnexis.com.ezproxy.umuc.edu/hottopics/lnacademic>; Dana Canedy and Nicholas Wade, "Florida Man Dies of Rare Form of Anthrax," *New York Times*, October 6, 2001, <http://www.nytimes.com/2001/10/06/us/florida-man-dies-of-rare-form-of-anthrax.html>.
8. J. A. Jernigan et al., "Bioterrorism-Related Inhalation Anthrax: The First Ten Cases Reported in the United States," *Emerging Infectious Diseases* 7, no. 6 (November–December 2001), <http://wwwnc.cdc.gov/eid/content/7/6/contents.htm>.
9. "FBI Begins Investigating Anthrax Cases," *USA Today*, October 9, 2001, <http://www.usatoday.com/news/attack/2001/10/09/anthrax.htm>.
10. "Fourth Case of Anthrax Is Identified; NBC Employee in N.Y. Tests Positive Weeks after Opening Letter from Fla.," *Washington Post*, October 13, 2001, <http://www.lexisnexis.com.ezproxy.umuc.edu/hottopics/lnacademic>.
11. Eric Lipton and Kirk Johnson, "Tracking Bioterror's Tangled Course," *New York Times*, December 26, 2001, <http://www.nytimes.com/2001/12/26/us/a-nation-challenged-the-anthrax-trail-tracking-bioterror-s-tangled-course.html?pagewanted=all>.
12. Vera Haller, "Third Anthrax Case at NY Post," *Newsday*, November 2, 2001, <http://www.ph.ucla.edu/EPI/bioter/thirdcaseNYPost.html>.
13. A. Freedman et al., "Cutaneous Anthrax Associated with Microangiopathic Hemolytic Anemia and Coagulopathy in a Seven-Month-Old Infant," *Journal of the American Medical Association* 287, no. 7 (2002): 869–74.
14. "CBS Anchor Dan Rather Comments on Anthrax Case," CNN, October 18, 2001, http://articles.cnn.com/2001-10-18/health/anthrax.CBS_1_anthrax-case-inhalation-anthrax-anthrax-diagnosis?_s=PM:HEALTH.
15. Greg B. Smith and Patrice O'Shaughnessy, "Anthrax Was Sent to NBC from Trenton FBI Finds Threatening Letter Mailed to Anchor," *New York Daily News*, October 14, 2001, <http://www.nydailynews.com/archives/news/anthrax-nbc-trenton-fbi-finds-threatening-letter-mailed-anchor-article-1.922400>.
16. "\$1 Million Offered for Information on Sender of Anthrax," *Washington Times*, <http://www.lexisnexis.com.ezproxy.umuc.edu/hottopics/lnacademic>.
17. William J. Broad and Denise Grade, "Science Slow to Ponder Ills That Linger in Anthrax Victims," *New York Times*, September 16, 2002, <http://www.nytimes.com/2002/09/16/us/threats-responses-victims-science-slow-ponder-ills-that-linger-anthrax-victims.html?pagewanted=all&src=pm>.
18. "N.J. Postal Worker Contemplates Action," *SouthJersey.com*, November 8, 2001, <http://www.southjersey.com/articles/?articleID=4685>.
19. Broad and Grade, "Science Slow to Ponder Ills."
20. Lena H. Sun, "Anthrax Patients' Ailments Linger, Fatigue, Memory Loss Afflict Most Survivors of October Attacks," *Washington Post*, April 20, 2002, <http://community.seattletimes.nwsources.com/archive/?date=20020421&slug=anthrax21>.
21. Alisa Ulferts and David Ballingrud, "Terror or Accidents? CDC FBI Investigate Lantana Case," *St. Petersburg Times*, October 5, 2001, http://www.sptimes.com/News/100501/State/Terror_or_accidents.shtml.
22. Gary Dorsey, "The Trials of a Citizen Soldier, Illness Lingers, Loyalty Wanes," *Baltimore Sun*, August 26, 2002, <http://www.baltimoresun.com/bal-to.anthrax26aug26,0,1033364.story>.
23. Michael Laris and Jennifer Lenhart, "Escaping the Grip of Anthrax, Va. Man Reflects on Deadly Struggle and Faces a Changed Life," *Washington Post*, December 6, 2001, <http://www.ph.ucla.edu/epi/bioter/escapinganthraxgrip.html>.
24. Kevin McCoy and Charisse Jones, "Case of N.Y. Anthrax Victim Intrigues Officials," *USA Today*, November 19, 2001, <http://www.usatoday.com/news/attack/2001/11/20/nguyen.htm>.
25. Lawrence K. Altman, "The Theories: Case in a Small Town Compounds Puzzle for Epidemiologists," *New York Times*, November 22, 2001, <http://www.nytimes.com/2001/11/22/nyregion/nation-challenged-theories-case-small-town-compounds-puzzle-for-epidemiologists.html?pagewanted=all>.
26. "Amerithrax Investigation Summary," Department of Justice, February 19, 2010, www.justice.gov/amerithrax, 2–3.
27. Ibid., 4–5.
28. Ibid., 5.
29. Ibid., 6.
30. Ibid.
31. Judith Miller and David Johnston, "A Nation Challenged: The Inquiry; Investigators Likened Anthrax in Leahy Letter to

That Sent to Daschle,” *New York Times*, November 20, 2001, <http://www.nytimes.com/2001/11/20/us/nation-challenged-inquiry-investigators-liken-anthrax-leahy-letter-that-sent.html?ref=anthrax>.

32. “Amerithrax Investigation Summary,” 5.
33. “Anthrax Scares Halt U.S. Congress,” *Toronto Star* <http://www.lexisnexis.com.ezproxy.umuc.edu/hottopics/lnacademic>.
34. “Amerithrax Investigation Summary,” 15.
35. Ibid.
36. “We Were Surprised It Was the Ames Strain,” *Frontline/PBS*, October 10, 2011, <http://www.pbs.org/wgbh/pages/frontline/criminal-justice/anthrax-files/paul-keim-we-were-surprised-it-was-the-ames-strain/>.
37. David Johnston and William J. Broad, “Anthrax in Mail Was Newly Made, Investigators Say,” *New York Times*, June 23, 2002, <http://www.nytimes.com/2002/06/23/us/anthrax-in-mail-was-newly-made-investigators-say.html?ref=anthrax>.
38. “Amerithrax Investigation Summary,” 12; Iver Peterson, “Testing Finds Some Traces of Anthrax in a Mailbox” *New York Times*, August 13, 2002, <http://www.nytimes.com/2002/08/13/nyregion/testing-finds-some-traces-of-anthrax-in-a-mailbox.html?ref=anthrax>.
39. “Amerithrax Investigation Summary,” 12. Peterson, “Testing Finds Some Traces.”
40. Faye Bowers, “Anthrax Case Hones in on Unusual Suspect: The FBI Narrows List of People It Wants to Interview to Thirty Scientists at Two Army Labs,” *Christian Science Monitor*, July 10, 2002, <http://www.csmonitor.com/2002/0710/p02s01-usju.html>.
41. Bowers, “Anthrax Case Hones in on Unusual Suspect.”
42. “Nixon Ends Biological Weapons Program,” *PBS*, <http://www.pbs.org/wgbh/americanexperience/features/general-article/weapon-nixon-ends/>.
43. Bowers, “Anthrax Case Hones in on Unusual Suspect.”
44. Ibid.
45. Joe Bauman, “Dugway Security Called Sloppy,” *Deseret News*, May 23, 2002, http://www.project-112shad-fdn.com/News_93.htm.
46. Ibid.
47. Bowers, “Anthrax Case Hones in on Unusual Suspect.”
48. Julian Borger, “Anthrax Killer ‘Could Grow More Bacteria,’” *Guardian*, <http://www.lexisnexis.com.ezproxy.umuc.edu/hottopics/lnacademic>.
49. Nicholas D. Kristof, “The Anthrax Files,” *New York Times*, July 12, 2002, <http://www.lexisnexis.com.ezproxy.umuc.edu/hottopics/lnacademic>; Borger, “Anthrax Killer ‘Could Grow More Bacteria.’”
50. Daniel Schorn, “Tables Turned in Anthrax Probe,” *60 Minutes*, February 11, 2009, <http://www.cbsnews.com/stories/2007/03/09/60minutes/main2552906.shtml>.
51. Ibid.
52. David Freed, “The Wrong Man,” *Atlantic Monthly*, May 2010, <http://www.theatlantic.com/magazine/archive/2010/05/the-wrong-man/8019/>.
53. Ibid., and David Johnston, “Apartment Searched Anew in F.B.I.’s Anthrax Inquiry,” *New York Times*, August 2, 2002, <http://www.nytimes.com/2002/08/02/us/apartment-searched-anew-in-fbi-s-anthrax-inquiry.html?ref=anthrax&pagewanted=print>. Don Foster, a professor of English at Vassar College who had aided the FBI in various cases through content analysis, and who published an article about Hatfill in *Vanity Fair* in 2002, told the FBI about his concerns, noting that few had the expertise and the access needed to carry out the attack. Barbara Hatch Rosenberg, a molecular biologist and former advisor to President Bill Clinton, independently came to the same conclusion that Hatfill was the perpetrator. She criticized the government for not making progress in the case and published a paper called “Possible Portrait of Anthrax Perpetrator” on the Web. She also met with lawmakers on Capitol Hill to alert them to her findings and urge that the FBI focus more heavily on Hatfill as a suspect.
54. “Amerithrax Investigation Summary,” 6.
55. Ibid.
56. Freed, “The Wrong Man.”
57. Ibid.
58. “Amerithrax Investigation Summary,” 6.
59. Johnston, “Apartment Searched Anew.”
60. “Statement of Hatfill,” *New York Times*, August 12, 2002, <http://www.nytimes.com/2002/08/12/us/weapons-expert-s-words.html?ref=anthrax&pagewanted=print>.

61. 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 Cyber H₂O

Key Questions

- ▶ **What are the main threats and vulnerabilities to the Curran-Gardner water plant?**
- ▶ **How long had the water pump behaved erratically?**
- ▶ **What caused the water pump to fail?**
- ▶ **What are the implications of the pump failure for the plant and the broader implications for the Water Sector?**

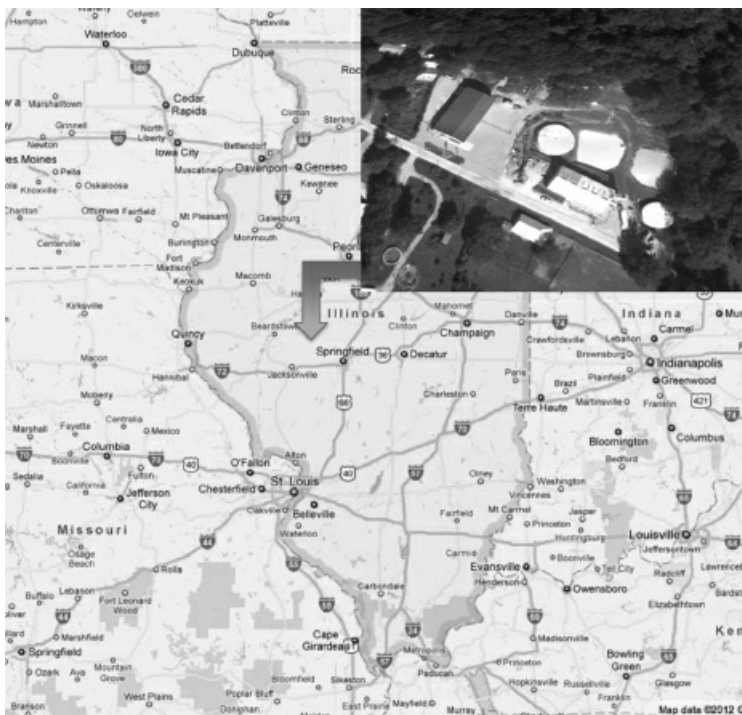
CASE NARRATIVE

On 8 November 2011, a Curran-Gardner Public Water District employee watched in disbelief as a large water pump repeatedly and spontaneously powered on and off. It was as if someone was repeatedly flipping an on/off switch. The Curran-Gardner facility serves the semi-rural townships of the same names that are situated in central Illinois, just west of the state capital of Springfield (see Map 3.1). Inside the facility, a supervisory control and data acquisition system (SCADA) that continuously monitors the plant alerted employees to the malfunctioning pump. Although the pump had been behaving strangely for two or three months, it had never turned on and off repeatedly.¹ By the end of the day the pump had burned out, leaving it unusable. Utility officials were flummoxed: Who or what had caused the pump failure?

The Nation's Water Sector: A Vital Resource

The Curran-Gardner Public Water District facility is part of the enormous and highly interdependent US Water Sector. The sector comprises more than 153,000 public drinking water and 16,500 public wastewater facilities that are principally owned and operated by the municipalities in which they are located. More than 84 percent of the US population receives its potable water from these facilities, and more than 75 percent receive wastewater services.²

Map 3.1 ▶ Location of the Curran-Gardner Public Water District Facility



Whether serving large municipalities or rural communities, drinking water facilities such as Curran-Gardner contain several key physical, cyber, and human elements that play a role in ensuring facility functionality (see Figure 3.1). The water must be located, transported, stored, treated, stored after treatment, distributed, and monitored for contaminants and flow volume. Plant operators and contractors oversee this process and are often aided by industrial control systems (ICS) such as supervisory control and data acquisition (SCADA) systems—usually Internet enabled—that help to monitor the complex workings of the utility and display it in a control room setting. Changes in any of the monitored plant activities are detected by the system, which brings the change to the attention of operators.³ The SCADA systems that oversee these plants are essential for early detection and mitigation of a host of potential problems, including mechanical malfunctions, power surges, water flow fluctuations, spikes in contaminants, and electric system shorts.

Water is a highly interdependent sector because it is vital to the successful functioning of many other sectors such as Agriculture, Emergency Services, the Defense Industrial Base, Communications, Energy, Transportation, Banking and Finance, the Chemical Industry, and Critical Manufacturing.⁴ All of these sectors depend on water to function. (See Figure 3.2.) Since 1950, overall water consumption in the United States has increased from 180 billion barrels a day to 410 billion barrels a day in 2005.⁵ Thermoelectric power is by far the biggest consumer of water in the country according to the US Geological Survey, but the water needs of the other sectors are no less vital.⁶

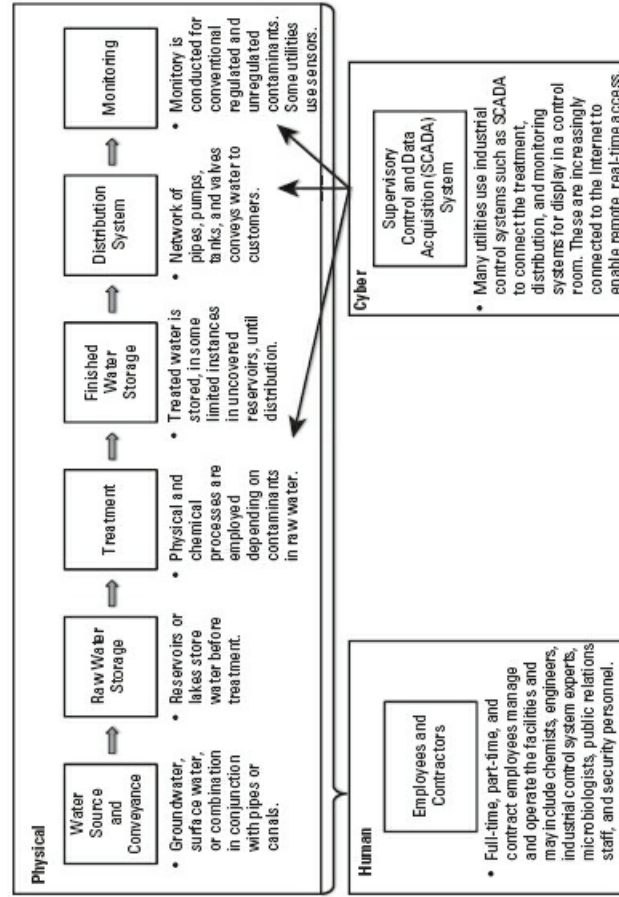
Growing Government Concerns

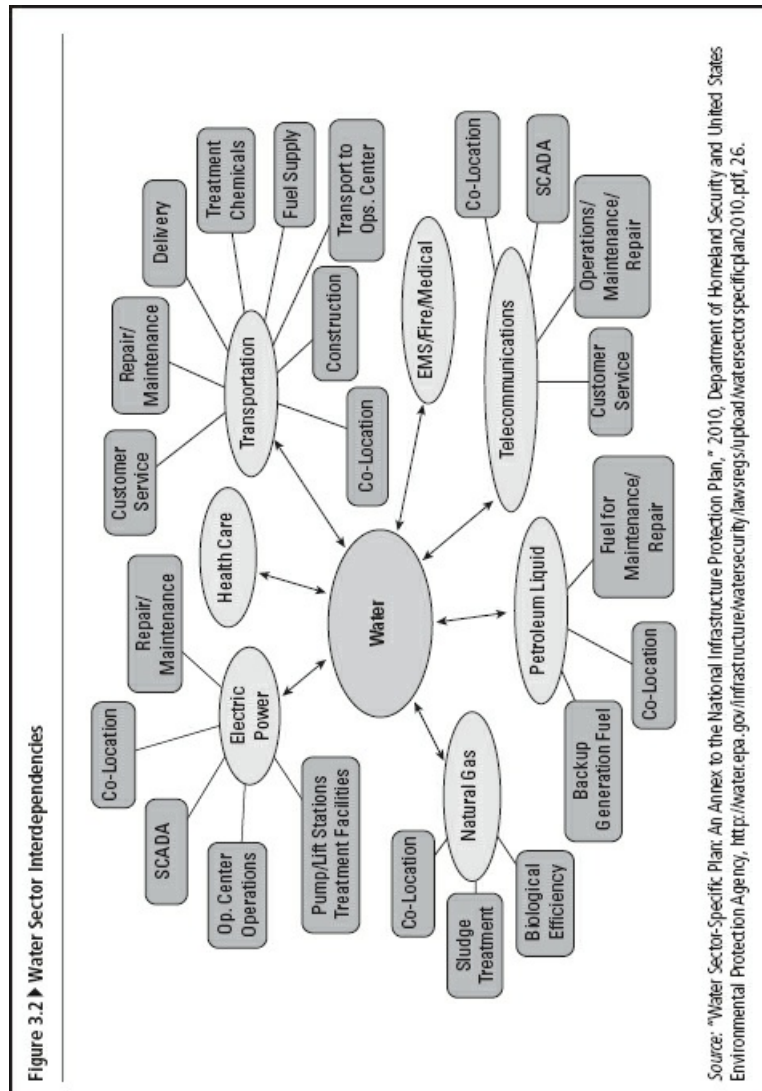
Over the past thirty years, the federal government increasingly has acted to protect this key resource and those who depend on it from both natural and human-made threats and vulnerabilities. The US Environmental Protection Agency (EPA) has gained stature as its

oversight and enforcement responsibilities have expanded commensurate with the government's increasing emphasis on protecting water resources. In the mid-1970s, the Safe Drinking Water Act established national drinking water standards. The Clean Water Act as revised in 1972 enacted water quality standards and enforcement authorities for the federal and state governments. Likewise, beginning in the 1990s and under the auspices of the amended Clean Air Act, the government required facilities that store certain chemicals, such as chlorine gas used in water facilities, to create risk management programs for submission to and oversight by the EPA.⁷

After the terrorist attacks of 11 September 2001, the federal government placed new emphasis on protecting the nation from human-made threats. In 2003, Homeland Security Presidential Directive 7 designated the EPA the federal lead, or sector-specific agency (SSA), for the Water Sector. In partnership with the US Department of Homeland Security (DHS), the EPA implements a variety of presidential directives, executive orders, and statutes, as well as helps to coordinate information sharing among federal, state, local, tribal, and industry stakeholders. In the intervening years, all levels of government and industry are participating in securing and improving the resilience—the ability to withstand natural disasters, human-made accidents, or attacks—of the US Water Sector. Together, these lead agencies coordinate across government sector partners via the Water Government Coordinating Council (GCC) and with private sector owners and operators via the Water Sector Coordinating Council (SCC) to encourage information sharing and analysis.

Figure 3.1 ► Physical, Cyber, and Human Components of Water Utilities





To ensure timely distribution of information, Congress established the Water Information Sharing and Analysis Center (WaterISAC) in 2002. This industry-staffed organization originally focused on contamination, terrorism, and cyber attacks, but it now distributes all-hazards information to the sector. In conjunction with state-level fusion centers, the ISAC's mandate is to provide timely alerts on water security, in addition to expert analysis of reported threats to water systems.⁸ State and urban area fusion centers around the country are also critical conduits of information between industry and the federal government. They "conduct analysis and facilitate information sharing, assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism."⁹ Although fusion centers are owned and operated by state and local entities, the federal government augments them with personnel and other resources.¹⁰

The goal of these efforts, according to the 2010 National Infrastructure Protection Plan (NIPP), is a Water Sector that is "secure and resilient ... and provides clean and safe water as an integral part of daily life, ensuring the economic vitality of and public confidence in the Nation's drinking water and wastewater service through a layered defense of effective preparedness and

security practices in the sector.”¹¹ The sheer size and openness of the system, as well as its distributed nature among independent operators, present a significant challenge for federal, state, and local homeland security professionals and businesses alike. Just a year before the pump failure in Illinois in 2011, the Department of Homeland Security finalized the Water Sector input to the NIPP, which spelled out four goals for the sector:

1. Sustain protection of public health and the environment.
2. Recognize and reduce risk.
3. Maintain a resilient infrastructure.
4. Increase communication, outreach, and public confidence.

Critical Infrastructure: The Cyber Dimension

As cyber attacks have grown in number and sophistication during the past decade and the nation’s critical infrastructures have become more dependent on the Internet, both the risks and potential consequences of cyber attacks on infrastructure targets have increased significantly. The 2003 National Strategy to Secure Cyberspace cited prevention of “cyber attacks against America’s critical infrastructures” as the first of three strategic cyber security objectives, including reduction of “national vulnerability to cyber attacks” and “minimiz[ing] damage from attacks that do occur.”¹² The National Cyberspace Policy Review released by the White House in 2008 further stressed that “cyberspace underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, and public safety,” adding that “a growing array of state and non-state actors are compromising, stealing, changing, or destroying information that could cause critical disruptions to U.S. systems.”¹³ The director of National Intelligence in 2009 said that the “growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures.”¹⁴

There is no formally agreed-upon lexicon used to describe these cyber activities. The US Department of Defense categorizes offensive computer network operations as either computer network exploitation (CNE) or computer network attack (CNA), although offensive operations often include elements of both.¹⁵ These terms are generally accepted both within and outside government to refer to the range of activities used to “attack, deceive, degrade, deny, disrupt, [and] exploit ... electronic information and infrastructure.”¹⁶ CNE includes information-gathering efforts, while CNA includes attacks that deny, disrupt, or degrade the target. Both are usually conducted under a deceptive cloak meant to obfuscate the source of the attack and include attack modes and outcomes that range from website defacements to distributed denial of service attacks, to code exploits that remotely control computers, machines, networks, and systems.

As the US government has taken steps toward a comprehensive strategy to protect cyberspace since 9/11, the tools at the command of insiders, foreign governments, and civilian hackers—the main threat groups, according to a recent study—are growing more sophisticated and better able to target the industrial control systems like SCADA that are vital components of US critical infrastructure, including the Water Sector.¹⁷ Recent government and industry-sponsored research projects have revealed significant vulnerabilities and the emergence of new

technologies that are increasing the risks to the industrial control systems that monitor and maintain key industries. These vulnerabilities are closely linked to the prevalence of aging systems and the lack of many basic security steps such as building firewalls or password protections. In a recent industry-sponsored study, hackers were able to break into six out of seven industrial control systems by exploiting hardware and software flaws such as backdoors that allowed hackers “to download or sidestep security completely.”¹⁸ In 2010, DHS noted the increased risk and recommended “placing all control system assets behind firewalls, using secure remote-access methods and disabling default passwords.”¹⁹

Box 3.1 LEXICON OF CYBER ATTACKS

The following activities represent, in ascending order of difficulty, many of the general types of offensive computer network operations currently observed in cyberspace.

Defacement: Altering a website or other online target for mischief or political purpose. Similar to graffiti.

DOS (Denial of Service)/DDOS (Distributed Denial of Service): The use of computers to deny access by visitors to a website or other online source. Can be done for commercial, criminal, political, or military purposes.

BOTS/Worms: Techniques to take command and control of one or more external computers remotely. Those computers can then be employed for various purposes, including DDOS attacks and ex-filtration of data.

Exploit: Penetration of a computer or computer network to identify, alter, or ex-filtrate data sets or code.

But even those systems that have security upgrades are still vulnerable to attack. In 2007, the DHS partnered with the power industry to conduct Project Aurora. The experiment demonstrated that hackers from the Idaho National Laboratory could remotely hack into an electric generator through the network and “by repeatedly triggering circuit breakers, [create] massive torque on the machinery, which eventually started to shake, smoke and tear itself to pieces.”²⁰ New technologies also allow hackers to map the system specifications of industrial control system networks, a capability that can be exploited to gain access to these systems. One technology is a search engine called Shodan. Since 2010, Shodan users have gathered such specifications on nearly 100 million devices, including their exact locations and operating software.²¹

Expanding Vulnerabilities Invite New Threats

As the government’s efforts to protect the Water Sector have intensified, so have the threats to the system. Prior to 9/11, the Water Sector’s main security focus was on natural threats such as weather or earthquakes, or human-made disruptions caused by vandalism or disgruntled insiders.²² After 9/11, concerns about potential threats to the system grew to include the possibility of chemical, biological, radiological, and nuclear attacks as well as cyber attacks. In

one 2006 report to Congress, the Congressional Research Service noted that

while some experts believe that risks to water systems actually are small, because it would be difficult to introduce sufficient quantities of agents to cause widespread harm, concern and heightened awareness of potential problems are apparent. Factors that are relevant to a biological agent's potential as a weapon include its stability in a drinking water system, virulence, culturability in the quantity required, and resistance to detection and treatment. Cyber attacks on computer operations can affect an entire infrastructure network, and hacking in water utility systems could result in theft or corruption of information or denial and disruption of service.²³

Experts have long cited the cyber dimension as a key vulnerability to critical infrastructure. In an open letter to President George W. Bush in 2002, a group of concerned scientists indicated that "the critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defense and the Internet, is highly vulnerable to cyber attack."²⁴ This is in large part because of the vulnerabilities inherent in the SCADA or other systems used to monitor and control them. According to Joe Weiss, an expert control systems engineer who is a frequent commentator on SCADA system vulnerabilities, what makes control systems like SCADA so effective also makes them vulnerable: they are designed to be accessed remotely by a number of different means, including the Internet.²⁵ In this way, these SCADA systems not only allow for easy remote monitoring and maintenance but also provide a door that can be used to mount intrusions. This vulnerability has been referred to by one expert as the "soft underbelly" of the Water Sector.²⁶

Adversaries are cognizant of these vulnerabilities. Several recent attacks suggest that hackers are exploiting these vulnerabilities with increasing frequency. The Federal Bureau of Investigation (FBI) in 2011 identified three cases that it described as "tease attacks" designed to highlight vulnerability of water systems as well as the prowess of the hacker.²⁷ During the same month that the Curran-Gardner incident occurred, a hacker named "pr0f" attacked a water system in Houston, Texas, defacing the website and posting screen shots of images allegedly obtained from inside the system.²⁸ Although the attack did not go beyond vandalism, the website defacement proved that "pr0f" had successfully breached the site's defenses and accessed protected information. Other attacks since 2000 have been far more destructive. In 2000, a disgruntled job applicant at a technology firm in Australia used a radio transmitter to access wastewater treatment plant controls remotely and release thousands of gallons of raw sewage into nearby rivers and parks with devastating results to local wildlife and waterways.²⁹

The DHS Industrial Control System Cyber Emergency Response Team (CERT) reports that water and power utilities are under daily attacks that are growing in number and sophistication.³⁰ CERT was established in 2002 to perform analysis, warning, information sharing, vulnerability reduction, mitigation, and national recovery efforts for critical infrastructure information systems.³¹ DHS-CERT staffs an operations center twenty-four hours a day and deploys fly-away teams to assist in network and forensic analysis when security incidents occur. Since 2009, CERT has seen a marked increase of reported incidents that range in sophistication from defacement to viruses, worms, and botnet attacks to exploits that CERT attributes to the espionage activities of state actors.³²

System Failure

On 8 November, Curran-Gardner plant operators did not immediately know the cause of the pump failure and took appropriate steps to investigate and report the incident to the EPA. The highly irregular failure came to the attention of the Illinois Statewide Terrorism and Intelligence Center—Illinois's fusion center. The fusion center learned that in the months preceding the attack there had been an anomalous access to the Curran-Gardner SCADA system via a Russian Internet protocol (IP) address using SCADA system log-on credentials. Attack attribution is a huge challenge for cyber analysis. This is because with the aid of authentic log-on credentials and the ability to bounce off multiple IP addresses, hackers are able to obfuscate the origins of the attack. Cyber forensics, however, can help unravel the mystery by pinpointing the location, time, and duration of an entry using the SCADA system log files. In this case, the fusion center learned about this foreign-based access to the system and realized that it could be done using stolen, or hacked, SCADA log-on credentials. By 10 November, the fusion center was increasingly convinced that it was dealing with a malicious, Russian-based cyber attack using stolen SCADA system log-on credentials. The fusion center knew that this type of malicious attack would be a first. Only two days after the water pump failure, on 10 November, the fusion center readied a report about the intrusion and the Russia connection and prepared it for release to federal, state, local, tribal, and industry stakeholders.

RECOMMENDED READINGS

- Copeland, Claudia. "Terrorism and Security Issues Facing the Water Infrastructure Sector." Congressional Research Service. December 15, 2010. <http://www.fas.org/sgp/crs/terror/RL32189.pdf>.
- "The National Strategy to Secure Cyberspace." The White House. February 2003. http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.
- "Water Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan." Department of Homeland Security and United States Environmental Protection Agency. 2010. <http://water.epa.gov/infrastructure/watersecurity/lawsregs/upload/watersectorspecificplan2010.pdf>.

Table 3.1 ▶ Case Snapshot: Cyber H₂O

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

CYBER H₂O

Structured Analytic Techniques in Action

Analysts are often asked to conduct their analyses under tight time frames on breaking issues. In situations when 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.

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 fusion 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?

STEP 2: What is the key question that needs to be answered?

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

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?

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.

- 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.
- 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?
- STEP 8:** Depending on responses to the previous questions, consider rewording the key question. Consider adding subordinate or supplemental questions.
- STEP 9:** Generate a list of potential sources or streams of reporting to be explored.
- 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.

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?

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 × 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 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.

STEP 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?

Table 3.2 ▶ Key Assumptions Check Template				
Key Assumption	Commentary	Solid	With Caveat	Unsupported

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.

Analytic Value Added. Which issues could undermine the analysis, and why?

NOTES

1. Kim Zetter, "H(ackers)2O: Attack on City Water Station Destroys Pump," *Wired*, November 18, 2011, <http://www.wired.com/threatlevel/2011/11/hackers-destroy-water-pump/>.
2. "Water: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan Executive Summary," Department of Homeland Security, May 2007, 3.
3. Robert O'Harrow Jr., "Cyber Search Engine Shodan Exposes Industrial Control Systems to New Risks," *New York Times*, June 3, 2012, http://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQA1K9KCV_story.html.
4. Water NIPP, 86.
5. J. F. Kenny, N. L. Barber, S. S. Hutson, K. S. Linsey, J. K., Lovelace, and M. A. Maupin, "Estimated Use of Water in the United States in 2005," U.S. Geological Survey Circular 1344, 2009, <http://pubs.usgs.gov/circ/1344/>.
6. Ibid.
7. Environmental Protection Agency website, <http://www.epa.gov/air/caa/>.
8. WaterISAC Water Security Network website, <https://portal.waterisac.org/web/aboutus.jspa>.
9. National Network of Fusion Centers Fact Sheet. Department of Homeland Security website, http://www.dhs.gov/files/programs/gc_1296484657738.shtm.
10. Ibid.
11. Water NIPP, 15.
12. "The National Strategy to Secure Cyberspace," The White House, February 2003, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.
13. "National Cyberspace Policy Review," The White House, 2008, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, iii.
14. Ibid., 1–2.
15. "Joint Publication 3–13 Information Operations," U.S. Department of Defense, February 13, 2006, http://www.fas.org/irp/doddir/dod/jp3_13.pdf, II-4 and II-5.
16. Ibid.
17. Edward Amoroso, *Cyber Attacks: Protecting National Infrastructure*. (Boston: Butterworth-Heinemann, 2010), 4–5.
18. O'Harrow, "Cyber Search Engine Shodan Exposes Industrial Control Systems."
19. Ibid.
20. Ibid.
21. Ibid.
22. Claudia Copeland and Betsy Cody, "Terrorism and Security Issues Facing the Water Infrastructure Sector," *Congressional Research Service*, updated May 24, 2006, <http://fpc.state.gov/documents/organization/68790.pdf>, 3.
23. Ibid., 3.

24. Open Letter from Concerned Scientists, *Frontline* website, February 2012, <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/letter.html>.
25. Joe Weiss, "Interview with Joe Weiss," *Frontline* website, <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/weiss.html>.
26. 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>.
27. Famed Y. Rashid, "FBI Admits Attackers Compromised SCADA Systems in Three U.S. Cities," *EWeek.com*, December 1, 2011, <http://www.eweek.com/c/a/Security/FBI-Admits-Attackers-Compromised-SCADA-Systems-in-Three-US-Cities-548815/>.
28. Ibid.
29. O'Harrow, "Cyber Search Engine Shodan Exposes Industrial Control Systems."
30. "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.
31. "Computer Network Security and Privacy Protection," Department of Homeland Security, February 19, 2010, http://www.dhs.gov/xlibrary/assets/privacy/privacy_cybersecurity_white_paper.pdf.
32. Ellen Messmer, "DHS: America's Water and Power Utilities under Daily Cyber-Attack," *Network World*, April 4, 2012, <http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html>.

4 Is Wen Ho Lee a Spy?

Key Questions

- ▶ Why did the US government prosecute Wen Ho Lee for spying?
- ▶ What are the strongest and weakest parts of the case?
- ▶ What may account for China's advances in nuclear technology?

CASE NARRATIVE

In the 1990s, as the administration of President Bill Clinton sought to expand diplomatic and trade relations with China, Chinese espionage against US technology targets—especially nuclear weapons data at national laboratories—received widespread publicity. As charges and countercharges surfaced, US scientists at Los Alamos (New Mexico) National Laboratory (LANL) who were studying Chinese nuclear tests concluded that a 1992 test demonstrated a sudden advance in the miniaturization of Beijing's nuclear warheads. They argued that the Chinese warhead was very similar to the United States' most advanced weapon, the W-88 (see Figure 4.1).¹ With this advance, the Chinese had the basis for a modern nuclear force.

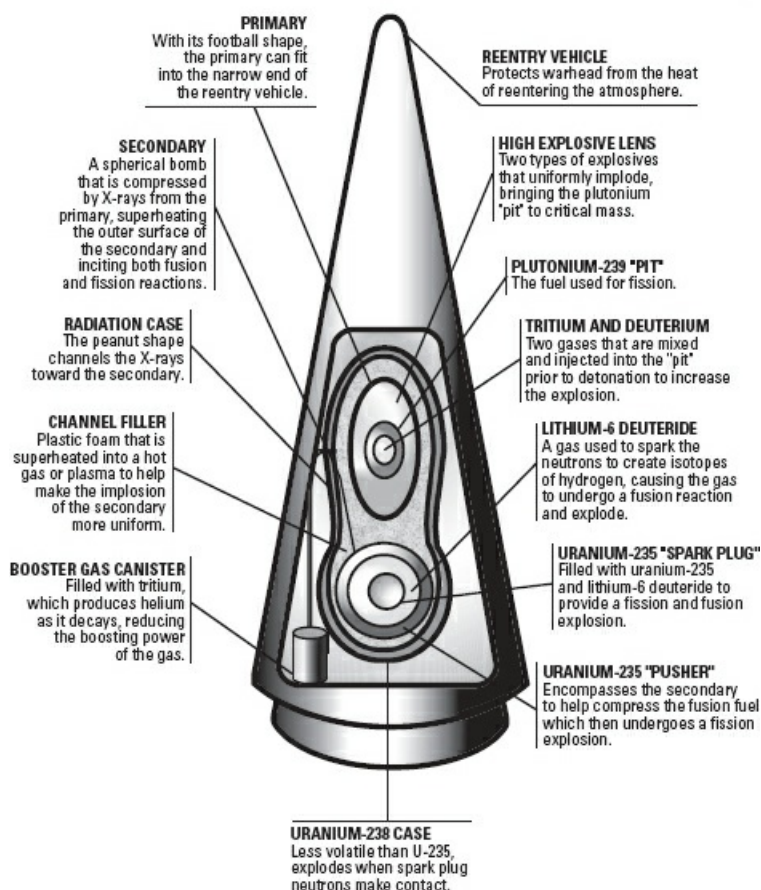
Robert M. Henson, a weapons designer at Los Alamos National Laboratory, believed that the only way the Chinese could have made such advances was by stealing US secrets.² Henson's view was seconded by John L. Richter, a bomb designer who specialized in creating the trigger for the hydrogen bomb. He argued that the sketchy evidence available pointed to the Chinese having acquired significant data on the trigger in the W-88.³ An investigation ensued, the results of which led investigators to believe that the theft of the W-88 data from the national laboratories occurred in the 1980s and that there was evidence of ongoing Chinese espionage at the increasingly open national laboratories in the 1990s. Given the small community of scientists with access to such data, investigators quickly focused on identifying who was responsible for the apparent leak.

The Chinese Threat

Counterintelligence officials report that China is aggressive at collecting information on US advanced technology.⁴ Beijing employs both soft—and mostly legal—as well as classic, hard spying techniques to gain access to critical information. Although the Chinese approach all scientists, they focus on ethnic Chinese, both from the mainland and from Taiwan.⁵ The Chinese informally collect tidbits from individuals in social settings, from Chinese visitors to US national laboratories and industrial sites, from scientific papers, and from Chinese students. In addition,

Chinese intelligence officials approach scientists traveling in China or attending scientific conferences. Beijing also employs classic spying techniques, recruiting spies and running double-agent operations.⁶

Figure 4.1 ▶ Schematic of the W-88 Nuclear Warhead



Source: Figure created by Nigah Ajaj, Pherson Associates, LLC. Adapted from Dan Stober and Ian Hoffman, *A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage* (New York: Simon & Schuster, 2007), 43.

The immediacy of the threat posed by Chinese espionage became apparent in 1995 after a critical piece of nuclear weapons intelligence came to the attention of Notra Trulock, director of intelligence at the Department of Energy (DOE).⁷ Henson shared with Trulock his concerns that China might have stolen nuclear secrets from the United States in the mid-1980s, although the theft had not been discovered until 1995.⁸ Henson was particularly concerned that China had managed to shrink the size of its warheads in a surprisingly short amount of time.⁹ The 1992 test had demonstrated that the Chinese could build missiles carrying multiple warheads and could now install them in submarines.¹⁰

The DOE Investigation: The Kindred Spirit Case

In the summer of 1995, DOE launched an assessment of China's nuclear weapons program as well as an administrative inquiry (AI) named Kindred Spirit to identify individuals within DOE who might have passed US nuclear secrets to the Chinese.¹¹ Trulock assembled a team, the Kindred Spirit Analytical Group (KSAG), to review the available data on Chinese bomb making.¹² The team found that the nuclear trigger ("primary") of the Chinese weapon was very similar in size and shape to that of the US W-88 warhead—one of the most sophisticated weapons in the US arsenal.

While the team was working this issue, it learned that an individual from mainland China had voluntarily provided classified Chinese documents to the Central Intelligence Agency (CIA) in June 1995.¹³ One document that attracted a lot of attention was a seventy-page paper that contained crude pictures, along with weights and measurements, of a variety of US weapons, including the W-88 warhead.¹⁴ Although much information about the W-88 was available in unclassified papers, certain details were not. The "walk-in" document described the outer measurements of the casing for the nuclear trigger.¹⁵ Former LANL Chief of Personnel and Information Security Robert Vrooman later recalled that the particular data referred to the engineering of the trigger, not to its design. According to Vrooman, if there had been espionage, it was not likely to have occurred at a design laboratory like LANL but in an engineering and production lab. In addition, the sketch of the W-88 in the walk-in document contained design flaws that had been added after the Los Alamos involvement.¹⁶

Trulock's team was unable to find a definitive link between the 1992 Chinese bomb test and the W-88. Team members were divided among three positions:

1. China had developed the new bomb on its own.¹⁷
2. China had benefited from a slow but steady accumulation of secrets over the years to develop its own miniaturized bomb.¹⁸
3. China had a master spy somewhere.¹⁹

Some knowledgeable scientists believed that the Chinese did not need to steal the data. They argued that as much as 99 percent of the data needed to build a weapon similar to the W-88 were available on the Internet.²⁰ There was also a possibility that China might have obtained the technology from another country, such as Russia. Following the demise of the Soviet Union, many Russian nuclear experts were marketing their skills around the world.²¹

KSAG eventually reached a consensus that the Chinese weapons program had been aided by espionage. Trulock was among those who were convinced that a spy at one of the National Defense laboratories had passed the design keys for the W-88 nuclear warhead to the Chinese.²² Trulock informally asked the Federal Bureau of Investigation (FBI) whether it would open an investigation at the end of the summer of 1995. The FBI declined, saying the case was too old and too cold and suggested that Trulock pursue the AI that he had launched in June.

Trulock assigned veteran investigators to undertake the inquiry, which began in November 1995. On the basis of the KSAG findings, the investigators were guided by three criteria for identifying suspects:

1. Individuals who had traveled to China between 1984 and 1988 (the period after final approval of the W-88 design and before the walk-in document)
2. Individuals with clearance to work with top-secret nuclear weapons data
3. Individuals who dealt with visiting delegations from China²³

The investigators quickly narrowed their search to LANL and the Lawrence Livermore National Laboratory (California) (LLNL).²⁴ They identified some seventy individuals at LANL who met some of the criteria and subsequently narrowed the list down to twelve who met all three criteria.²⁵ Trulock and his team quickly honed in on one individual, Wen Ho Lee, a nuclear weapons specialist at LANL.²⁶

Some officials would later question the list as inconsistent and unreliable. For example, it included only those individuals whose travel expenses were paid by DOE. The short list included three individuals who had no access to classified data and one with no clearance.²⁷ DOE's acting chief of counterintelligence recommended that the case be closed for lack of evidence, but it remained active.

In May 1996, DOE completed its AI and submitted its report to the FBI. The central message of the report was that espionage had occurred and the most likely source was at LANL.²⁸ The report named LANL scientist Wen Ho Lee and his wife, Sylvia, as the most logical suspects, noting that Lee was the only target who had opportunity, motive, and legitimate access.²⁹ Lee had traveled to China twice during the specified time frame, in 1986 and 1988.³⁰ Both times, he had received DOE approval to attend scientific conferences. He possessed a Q clearance, which gave him access to all classified material in his field at LANL. He and Sylvia had met visiting Chinese delegations frequently, she eagerly acted as an interpreter for the Chinese visitors, and she accompanied Lee on his two trips to China.³¹



Wen Ho Lee pictured with his daughter, Alberta Lee.

Wen Ho Lee's Background

Wen Ho Lee was born in Nantou, Taiwan, on 21 December 1939. He received a BS degree from National Cheng Kung University in Taiwan. Lee came to the United States in 1964 and became a

citizen in 1974. He earned a PhD in mechanical engineering from Texas A&M University in 1970 and was hired by LANL as a research mathematician in 1978. In 1980, he joined the X Division, where nuclear weapons are designed. His job was to create computer codes that modeled the fluid-like movement of explosions and to archive any related information developed. Scientists used these computer programs in nuclear weapons design and nuclear test simulations.³²

Lee made professional and personal trips to China and to Taiwan.³³ During the 1980s, he traveled twice to China. In 1986, he delivered a paper at a scientific conference in Beijing.³⁴ Two years later, he attended another conference in Beijing.³⁵ During the conference, Lee met with Hu Side and another Chinese scientist in a Beijing hotel room.³⁶ Hu was head of the Chinese Academy of Engineering Physics—the Chinese bomb makers—and the designer of the two-point nuclear bomb trigger. At the meeting, Hu asked Lee how to make a smaller hydrogen bomb using an oval-shaped fuel case. Later, Lee said that he did not answer the question.³⁷

During the 1980s, Wen Ho Lee became an FBI informant.³⁸ He reportedly provided useful information on at least one case under investigation.³⁹ His wife, Sylvia Lee, was a secretary at LANL, where she helped entertain visiting Chinese scientists and provided tours of local sights.⁴⁰ She also was a research contact for Chinese scientists. In 1985, Sylvia Lee was invited to speak at a Beijing conference on sophisticated computers, even though she was only a secretary. Wen Ho Lee attended the conference with his wife.⁴¹ In 1987, she became an informant to the FBI on the Chinese delegations she met with at LANL.⁴² During these years, there was no significant change in the lifestyle of Wen Ho Lee or his wife.⁴³

Lee did not report all his contacts with Chinese scientists at the 1988 conference or other conferences he attended.⁴⁴ The absence of reports by Lee was noted by LANL security chief Vrooman.⁴⁵ Lee admitted to investigators that he had unauthorized contacts with Chinese scientists over the years.

Lee first came to the attention of investigators in December 1982, when he was overheard on a wiretap making a phone call to a Taiwanese American scientist who was suspected of providing the Chinese with neutron bomb secrets from LLNL.⁴⁶ During the phone call, Lee offered to help find out who had “squealed on” the scientist.⁴⁷ Although no indictment of the suspect scientist was issued in what the FBI called the Tiger Trap case⁴⁸ because of insufficient evidence, the suspect was fired from LLNL.⁴⁹ Lee denied making the call until investigators looking into the Tiger Trap case confronted him with evidence of the conversation.⁵⁰ He also explained to investigators that he gave Taiwanese officials unclassified documents on nuclear reactor safety but that he had not told US government officials at the time, as required by security regulations.⁵¹

Lee made two trips to Taiwan in the 1990s. In 1994, he traveled to Hong Kong, a trip that he did not report to security officials as required.⁵² Investigators later found that he made two credit card purchases at a Hong Kong travel agency. One purchase was for \$100 and one for \$700.⁵³ Investigators report that \$700 would have covered the purchase of an airplane ticket to Shanghai.⁵⁴ Lee traveled to Taiwan in 1998, where he had been putting out feelers for jobs.⁵⁵ During March and April of that year, he spent six weeks at the Chung Shan Military Institute in Taiwan, where he received a fee of about \$5,000. While in Taiwan, Lee called the LANL computer help desk to ask if could access the classified computer at the lab. He was told that he could not access the classified system from Taiwan. Investigators later learned that he had

downloaded an unclassified computer code from LANL to his computer in Taiwan.⁵⁶ In December 1998, Lee traveled for three weeks to Taiwan, and a private Taiwanese company paid for the trip.⁵⁷

In 1994, Wen Ho Lee attended a party at Los Alamos for visiting Chinese scientists even though he was not on the invitation list.⁵⁸ During the party, Hu Side greeted Lee warmly. Some sources report that Hu hugged Lee.⁵⁹ According to a translator at the party, Hu thanked Lee for computer software and calculations on hydrodynamics Lee had supplied. Hu added that the information had aided China greatly.⁶⁰

The FBI Investigation

In May 1996—two days after receiving the DOE report—the FBI agreed to open an investigation based on DOE’s administrative inquiry.⁶¹ With a full case load, the local agent had only limited time to devote to Kindred Spirit. As a result, no agent worked full time on the case.⁶²

In April 1997, Lee brought himself to the attention of the FBI by submitting a standard request to hire a postdoctoral researcher who happened to be a Chinese citizen. Lee said he needed an assistant to help with his work on codes used to model some aspects of nuclear weapons tests. This spurred the FBI to request an electronic surveillance warrant under the Foreign Intelligence Surveillance Act (FISA).⁶³

The FBI wanted to monitor Lee’s contacts with his graduate student. Over the summer of 1996, the FBI presented three separate drafts of its request for a FISA warrant to the Department of Justice (DOJ). DOJ took the unusual step of denying the FBI request in August 1997, citing a lack of “probable cause” that Lee was a spy.⁶⁴ The FISA request could not demonstrate a link between the theft of the W-88 design and Lee. DOJ was also disturbed by the failure to investigate other possible suspects.⁶⁵

FBI director Louis J. Freeh appreciated the anxiety of DOE over Lee’s continuing presence in the X Division and his access to nuclear secrets. After a top-level review, the FBI concluded it did not have sufficient evidence to arrest Lee, but there was no reason to leave Lee in place.⁶⁶ Miscommunications among FBI headquarters, LANL, and DOE headquarters, however, resulted in Lee staying in his job.⁶⁷

Little progress was made on the investigation in 1997 and 1998. Neither the FBI nor DOE knew that Lee had left the country during March and April 1998 to work as a consultant at a nuclear weapons research institute in Taiwan.⁶⁸ Since LANL was not paying for the trip, Lee was not required to ask for permission. The FBI initiated a “false flag” operation in August 1998 in which FBI agents posing as Chinese officials sought to recruit Lee. Lee rebuffed them, but he did not report the pitch to his superiors as required.⁶⁹

The case did not get much attention until later in 1998, when two House committees conducted hearings on Chinese nuclear activities. US–China relations had been politically charged for many years.⁷⁰ The Reagan administration had expanded scientific exchanges with China and declassified millions of documents relating to nuclear arms. Washington had also encouraged weapons specialists to exchange unclassified information with foreign counterparts.⁷¹ The Clinton administration had continued to expand ties with China.⁷² In 1994, national labs were no longer required to conduct background checks on foreign⁷³ scientists visiting the labs for scientific exchanges.⁷⁴ Republicans charged that the Clinton White House

was downplaying Chinese spying because it conflicted with the administration's drive for a greater strategic and commercial partnership with Beijing. President Clinton had already eased the sale of supercomputers and satellite technology to China.⁷⁵

The House Permanent Select Committee on Intelligence (HPSCI) in 1998 requested an update on the W-88 Chinese espionage case from DOE.⁷⁶ Meanwhile, a special House committee, headed by Rep. Christopher Cox (R-CA), was conducting hearings on the transfer of technology to China and had begun to focus on suspected Chinese nuclear espionage. Trulock testified before the Cox Committee in November 1998 that the Chinese had stolen the design of the W-88. In December, the FBI told the committee that the Chinese had probably penetrated US weapons laboratories and that a suspected spy was still unexposed at LANL, with his security clearances unchanged. At the time, Lee was in Taiwan on a trip approved by DOE.⁷⁷

Polygraph Results and the Missing Computer Files

Information on Chinese nuclear espionage at the national laboratories began leaking to the press from the Cox Committee from December 1998 into early 1999. DOE decided to interview and polygraph Lee after his return from Taiwan in late December 1998.⁷⁸ During the 23 December interview, Lee admitted that he had met with two Chinese scientists interested in miniaturized nuclear bombs in his hotel room during a visit to Beijing in 1988. He claimed that he told the Chinese that he didn't know the answer and refused to discuss the issue with them. When asked why he did not report the meeting at the time, Lee said he forgot.⁷⁹ Lee did not go home after this meeting but made several attempts to enter the X Division after his access was suspended, including an unauthorized visit to the laboratory at 0330 on Christmas Eve. He succeeded in entering X Division on two occasions. DOE subsequently assigned Lee to another department, T Division.⁸⁰

FBI and DOE forensic specialists discovered that Lee had transferred a large number of files from a classified to an unclassified part of LANL's computer system.⁸¹ According to press reports, Lee maintained that he had been instructed to archive the bomb data.⁸² Lee had begun the transfers as early as 1988⁸³ but made the bulk of them in 1993. In fact, the bulk of the downloads occurred in 1993 and 1994.⁸⁴ Lee told a fellow scientist at Los Alamos that he needed to transfer the files from a classified computer to an unclassified computer because the classified computer did not have tape drives and he could not download files from it directly. At the time of the downloads in 1993, Lee learned that he might be laid off from LANL because of budget cuts.⁸⁵ Investigators later found seven letters dated 1993 and 1994 on Lee's home computer addressed to universities and institutes and inquiring about job prospects, but there was no evidence that the letters had been mailed.⁸⁶

The FBI believed that Lee had transferred files from a classified to an unclassified system and downloaded them onto tapes. The computer index confirmed that he had downloaded all the files he had transferred.⁸⁷ The contents of a tenth tape, copied in 1997,⁸⁸ were never transferred to the unclassified system because Lee's X Division computer had a tape drive by then. LANL experts told the FBI that the later tape contained up-to-date information that would have made the 1993-94 tapes more useful. Lee at first denied making the tapes,⁸⁹ but when confronted with the list, he admitted that there had been tapes. He denied any criminal intent in making the tapes. Wen Ho Lee last downloaded information from the classified computer system to the tape drive on his own classified computer in 1997.⁹⁰ The case had morphed from a counterintelligence

investigation to a possible criminal case.

The transferred files did not include user manuals for the computer codes.⁹¹ The 1993–94 transfers took nearly forty hours over seventy days.⁹² The transfers were neither quick nor easy to do, requiring numerous deliberate steps to move data from the secure partition to the open partition of the system.⁹³ Lee left some files on the open system for as long as six years.⁹⁴ When LANL computer experts looked for the files, however, they found Lee had deleted them. In fact, he had been busy since the polygraph of 23 December 1998, trying to gain physical access to X Division and to his X Division computer account. In all, he deleted 360 files—some 800 megabytes or 450,000 pages of data.⁹⁵ Agents found materials in his office desk that included handwritten Chinese-language notes on how to download codes used to develop various nuclear weapons, including the W-88.⁹⁶ They also found documents on Lee’s desk with the classification markings removed. But there was no direct evidence that Wen Ho Lee had ever passed or tried to pass any classified national security information to China.⁹⁷

Over the next several months, the FBI conducted an exhaustive computer network analysis in an effort to discover the contents of the files Lee had transferred, downloaded, and deleted.⁹⁸ The FBI was able to recover three of the tapes from Lee’s T Division office,⁹⁹ but seven remained missing.¹⁰⁰ Lee told the FBI that he had destroyed them. He gave no explanation for why he had made the tapes or why and how he had disposed of them. He denied taking them home.

After the FBI identified the deleted files, it turned to experts at DOE and LANL to determine their value. Lee apparently had downloaded almost all of LANL’s nuclear weapons source codes and other files, which together provided the means for computer-simulated tests of nuclear weapons.¹⁰¹ Substantial amounts of the material Lee had downloaded were classified as PARD, which stands for “Protect as Restricted Data.” Such data are controlled, but at that time a determination had not been made as to whether they were classified. PARD is often applied to large volumes of data such as computer printouts, much of which are unclassified. During Lee’s investigation, some of the PARD material was later reclassified as “Confidential” and “Secret.”¹⁰²

Officials at the FBI placed a new emphasis on the case in early 1999.¹⁰³ When they interviewed Lee in January, he provided previously unknown information about contacts he had made with Chinese scientists in the 1980s, including a meeting with Hu Side.¹⁰⁴ The FBI interviewers were satisfied with Lee’s responses and were prepared to clear him, but they still wanted to see the results of the DOE polygraph. After some delay, they obtained the results of the polygraph, which cleared Lee. Later that month, FBI specialists discovered problems with the polygraph and questioned its results. In February Lee underwent an FBI polygraph interview, which he failed.¹⁰⁵ He returned to his office, where he told a supervisor that he had failed the polygraph and that he might have inadvertently passed classified information to a foreign country.¹⁰⁶

The FBI stepped up its investigation in early March, when it learned that the *New York Times* was preparing an article about an espionage investigation involving an unidentified LANL scientist.¹⁰⁷ The FBI interviewed Lee, who could not explain the differences between the travel report following his 1988 visit to China and the information he had given to investigators after his polygraphs.¹⁰⁸ Lee consented to a search of his office computers¹⁰⁹ but not to a search of his home.¹¹⁰

The Case Goes Public

A *New York Times* article on 6 March 1999 reported that nuclear secrets stolen from a US government laboratory had enabled China to make a leap in nuclear weapons development: the miniaturization of its bombs.¹¹¹ It said there was a suspect, a Chinese American scientist at Los Alamos.¹¹² It cited comments by unidentified officials that the White House had minimized the espionage investigation for political reasons. One official said that exposing the espionage would undercut the administration's efforts to have a strategic partnership with China.¹¹³

Once the case against Wen Ho Lee surfaced publicly, his defenders charged that he was singled out for investigation because he was Chinese American.¹¹⁴ Charges of racial profiling became a key element in his defense. Additionally, his defense claimed that there was no definitive evidence that Wen Ho Lee passed data to the Chinese¹¹⁵ or any proof of theft.¹¹⁶ In this politically charged atmosphere, many commentators believed that politics drove the prosecution of Wen Ho Lee for espionage and produced intense pressure for prosecutors to bring home a conviction.

Lee the Spy?

On Monday, 8 March 1999, Lee was fired after nearly twenty years at LANL on orders of Secretary of Energy Bill Richardson.¹¹⁷ Richardson ordered a tightening of security at all the national laboratories, including reinstating background checks for foreign scientists visiting the laboratories from sensitive countries.¹¹⁸ On 10 December 1999, Lee was indicted on fifty-nine counts of illegally removing highly classified information from LANL.¹¹⁹ Wen Ho Lee was jailed in January 2000 and held in solitary confinement.¹²⁰ He ultimately pled guilty to one count of mishandling a controlled document, was sentenced to time served, and was released in September 2000.¹²¹ At the time of his release, Wen Ho Lee agreed to undergo sixty hours of debriefing, under oath, by the government. During the debriefing, Lee acknowledged making as many as a dozen trips to Taiwan during the previous twenty years—more than officials previously knew about—but the purpose of the trips was not clear. Lee insisted that he threw the missing tapes into the trash; they have never been found.¹²²

RECOMMENDED READINGS

Lee, Wen Ho. *My Country versus Me: The First-Hand Account by the Los Alamos Scientist Who Was Falsely Accused of Being a Spy*. With Helen Zia. New York: Hyperion, 2002.

Stober, Dan, and Ian Hoffman. *A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage*. New York: Simon & Schuster, 2007.

Trulock, Notra. *Code Name Kindred Spirit: Inside the Chinese Nuclear Espionage Scandal*. San Francisco: Encounter Books, 2003.

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

IS WEN HO LEE A SPY?

Structured Analytic Techniques in Action

Is Wen Ho Lee a spy? When the stakes are this high, it is important to ensure that all the data have been considered from every possible angle before rendering a judgment. The following combination of techniques—Force Field Analysis, Deception Detection, Premortem Analysis, and Structured Self- Critique—can be used in concert to examine the case of Wen Ho Lee and the possibility that he is a spy, or not.

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 a form of brainstorming to identify the main factors that will influence the issue.

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.

Table 4.2 ▶ Force Field Analysis Template			
Issue: Wen Ho Lee Is a Chinese Spy			
Weight	Arguments For	Arguments Against	Weight
Total			Total

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.

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

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?

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.

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 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 4.3 ▶ When to Use Deception Detection

Analysts should be concerned about the possibility of deception when:

The potential deceiver has a history of conducting 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.

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 the new information would cause the Intelligence Community, the US government, or the client to expend or divert significant resources.

The potential deceiver may have a feedback channel that illuminates whether and how the deception information is being processed, and to what effect.

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 as your guide.

Table 4.4 ▶ Deception Detection Templates

Motive, Opportunity, and Means (MOM)	
Motive: What are the goals and motives of the potential deceiver?	
Channels: What means are available to the potential deceiver to feed information to us?	
Risks: What consequences would the adversary suffer if such a deception were revealed?	
Costs: Would the potential deceiver need to sacrifice sensitive information to establish the credibility of the deception channel?	
Feedback: Does the potential deceiver have a feedback mechanism to monitor the impact of the deception operation?	
Past Opposition Practices (POP)	
Does the adversary have a history of engaging in deception?	
Does the current circumstance fit the pattern of past deceptions?	
If not, are there other historical precedents?	
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?	
What is the basis for judging the source to be reliable?	
Does the source have direct access or only indirect access to the information?	
How good is the source's track record of reporting?	
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?	
Evaluation of Evidence (EVE)	
How accurate is the source's reporting? Has the whole chain of evidence, including translations, been checked?	
Does the critical evidence check out? Remember, the subsource can be more critical than the source.	
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)?	
Do other sources of information provide corroborating evidence?	

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.

Technique 3: The Premortem Analysis and Structured Self-Critique

The goal of these techniques¹²³ 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.

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.
- 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.
- 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?
- 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?
- STEP 5:** Is there any contradictory or anomalous information? Was any information overlooked that is inconsistent with the lead hypothesis?
- STEP 6:** Is there a potential for deception? Does anyone have motive, opportunity, and means to deceive you, either intentionally or unintentionally?
- STEP 7:** Is there an absence of evidence, and does it influence the key judgment?
- 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.)
- 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.

Analytic Value Added. As a result of your analysis, would you retain, add a caveat to, or dismiss the mainline judgment, and why?

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.

NOTES

1. James Risen and Jeff Garth, "Breach at Los Alamos: A Special Report; China Stole Nuclear Secrets for Bombs, US Aides Say," *New York Times*, March 6, 1999, <http://www.nytimes.com/1999/03/06/world/breach-los-alamos-special-report-china-stole-nuclear-secrets-for-bombs-us-aides.html>.

2. Matthew Purdy, "The Prosecution Unravels: The Case of Wen Ho Lee," with James Stern Gold, *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. Ibid.

4. Ibid.

5. Ibid.

6. Risen and Garth, "Breach at Los Alamos."

7. Purdy, "The Prosecution Unravels."

8. Ibid.

9. Ibid.

10. Ibid.
11. Ibid.
12. Ibid.
13. Risen and Garth, "Breach at Los Alamos."
14. Ibid.
15. Purdy, "The Prosecution Unravels."
16. Robert Schemer, "What's Left of Case against Lee? Not Much," *Los Angeles Times*, December 14, 1999, <http://articles.latimes.com/1999/dec/14/local/me-43741>.
17. Purdy, "The Prosecution Unravels."
18. Ibid.
19. Ibid.
20. William J. Broad, "Ideas and Trends: Bombshells; Are There Any Nuclear Secrets Left to Steal?" *New York Times*, September 3, 2000, <http://www.nytimes.com/2000/09/03/weekinreview/ideas-trends-bombshells-are-there-any-nuclear-secrets-left-to-steal.html>.
21. Risen and Gerth, "Breach at Los Alamos."
22. Purdy, "The Prosecution Unravels."
23. James Risen and David Johnston, "US Will Broaden Investigation of China Nuclear Secrets Case," *New York Times*, September 23, 1999, <http://www.nytimes.com/1999/09/23/us/us-will-broaden-investigation-of-china-nuclear-secrets-case.html>.
24. Purdy, "The Prosecution Unravels."
25. Risen and Johnston, "US Will Broaden Investigation."
26. Risen and Gerth, "Breach at Los Alamos."
27. James Sterngold, "US to Reduce Case against Scientist to a Single Charge," *New York Times*, September 11, 2000, <http://www.nytimes.com/2000/09/11/us/us-to-reduce-case-against-scientist-to-a-single-charge.html>.
28. Purdy, "The Prosecution Unravels."
29. Ibid.
30. Ibid.
31. Ibid.
32. Ibid.
33. Ibid.
34. Jeff Gerth and James Risen, "1998 Report Told of Lab Breaches and China Threat," *New York Times*, May 2, 1999, <http://www.nytimes.com/1999/05/02/world/1998-report-told-of-lab-breaches-and-china-threat.html>.
35. Ibid.
36. David Johnston, "Suspect in Loss of Nuclear Secrets Unlikely to Face Spying Charges," *New York Times*, June 15, 1999, <http://www.nytimes.com/1999/06/15/world/suspect-in-loss-of-nuclear-secrets-unlikely-to-face-spying-charges.html>.
37. Purdy, "The Prosecution Unravels."
38. Gerth and Risen, "1998 Report Told of Lab Breaches."
39. James Risen and Jeff Gerth, "US Says Suspect Put Code on Bombs in Unsecure Files," *New York Times*, April 28, 1999, <http://www.nytimes.com/1999/04/28/world/us-says-suspect-put-code-on-bombs-in-unsecure-files.html>.
40. Risen and Gerth, "Breach at Los Alamos."
41. Ibid.
42. Risen and Gerth, "US Says Suspect Put Code on Bombs in Unsecure Files."
43. Johnston, "Suspect in Loss of Nuclear Secrets Unlikely to Face Spying Charges."
44. Ibid.
45. Purdy, "The Prosecution Unravels."
46. Jeff Gerth and James Risen, "A Visit from China: New Spy Case; Intelligence Report Points to 2nd China Nuclear Leak," *New York Times*, April 8, 1999, <http://www.nytimes.com/1999/04/08/world/visit-china-new-spy-case-intelligence-report-points-2d-china-nuclear-leak.htm>; Gerth and Risen, "1998 Report Told of Lab Breaches and China Threat."
47. Purdy, "The Prosecution Unravels."
48. Ibid.
49. Gerth and Risen, "1998 Report Told of Lab Breaches and China Threat."
50. Purdy, "The Prosecution Unravels."
51. Ibid.
52. Risen and Gerth, "Breach at Los Alamos."
53. Ibid.; Johnston, "Suspect in Loss of Nuclear Secrets Unlikely to Face Spying Charges."
54. Risen and Gerth, "Breach at Los Alamos"; Johnston, "Suspect in Loss of Nuclear Secrets Unlikely to Face Spying

Charges.”

55. Purdy, “The Prosecution Unravels.”
56. Ibid.
57. Ibid.
58. Ibid.
59. Gerth and Risen, “1998 Report Told of Lab Breaches and China Threat.”
60. Purdy, “The Prosecution Unravels.”
61. Ibid.
62. Risen and Gerth, “Breach at Los Alamos.”
63. The Foreign Intelligence Surveillance Act (1978) sets in place procedures for the FISA court to approve requests from the FBI to conduct physical and/or electronic surveillance of US persons and on US territory.
64. James Risen and Jeff Gerth, “China Spy Suspect Reportedly Tried to Hide Evidence,” *New York Times*, April 30, 1999, <http://www.nytimes.com/1999/04/30/world/china-spy-suspect-reportedly-tried-to-hide-evidence.html>; Gerth and Risen, “1998 Report Told of Lab Breaches and China Threat.”
65. Purdy, “The Prosecution Unravels.”
66. Risen and Gerth, “Breach at Los Alamos.”
67. Gerth and Risen, “1998 Report Told of Lab Breaches and China Threat”; Risen and Gerth, “Breach at Los Alamos.”
68. Purdy, “The Prosecution Unravels.”
69. Gerth and Risen, “1998 Report Told of Lab Breaches and China Threat.”
70. Purdy, “The Prosecution Unravels.”
71. Ibid.
72. Ibid.
73. Ibid.
74. Risen and Gerth, “Breach at Los Alamos.”
75. Ibid.
76. Ibid.
77. Ibid.
78. Ibid.
79. Purdy, “The Prosecution Unravels.”
80. Risen and Gerth, “1998 Report Told of Lab Breaches and China Threat.”
81. Ibid.; Risen and Gerth, “US Says Suspect Put Code on Bombs in Unsecure Files.”
82. Gerth and Risen, “1998 Report Told of Lab Breaches and China Threat”; Purdy, “The Prosecution Unravels.”
83. Purdy, “The Prosecution Unravels.”
84. James Risen, “Officials Describe Loss of Nuclear Secrets at Los Alamos,” *New York Times*, December 12, 1999, <http://www.nytimes.com/1999/12/12/us/officials-describe-loss-of-nuclear-secrets-at-los-alamos.html>.
85. Purdy, “The Prosecution Unravels.”
86. Ibid.
87. Janet Reno and Louis J. Freeh, “Excerpts from Testimony at Hearing on the Wen Ho Lee Case,” *New York Times*, September 27, 2000, <http://www.nytimes.com/2000/09/27/us/excerpts-from-testimony-at-hearing-on-the-wen-ho-lee-case.html>.
88. Risen, “Officials Describe Loss of Nuclear Secrets at Los Alamos.”
89. Purdy, “The Prosecution Unravels.”
90. Risen, “Officials Describe Loss of Nuclear Secrets at Los Alamos.”
91. Purdy, “The Prosecution Unravels: The Case of Wen Ho Lee.”
92. Reno and Freeh, “Excerpts from Testimony at Hearing on the Wen Ho Lee Case.”
93. Risen, “Officials Describe Loss of Nuclear Secrets at Los Alamos.”
94. Reno and Freeh, “Excerpts from Testimony at Hearing on the Wen Ho Lee Case.”
95. Ibid.
96. Purdy, “The Prosecution Unravels.”
97. Johnston, “Suspect in Loss of Nuclear Secrets Unlikely to Face Spying Charges.”
98. Purdy, “The Prosecution Unravels.”
99. Risen, “Officials Describe Loss of Nuclear Secrets at Los Alamos.”
100. David Johnston and James Risen, “The Los Alamos Secrets Case: The Overview; Nuclear Weapons Engineer Indicted in Removal of Data,” *New York Times*, December 11, 1999, <http://www.nytimes.com/1999/12/11/us/los-alamos-secrets-case-overview-nuclear-weapons-engineer-indicted-removal-data.html>.
101. Risen and Gerth, “US Says Suspect Put Code on Bombs in Unsecure Files.”

102. William J. Broad, "Files in Question in Los Alamos Case Were Reclassified," *New York Times*, April 15, 2000, <http://www.nytimes.com/2000/04/15/us/files-in-question-in-los-alamos-case-were-reclassified.html>.
103. Purdy, "The Prosecution Unravels."
104. Ibid.
105. Risen and Gerth, "Breach at Los Alamos."
106. Broad, "Files in Question."
107. Purdy, "The Prosecution Unravels."
108. James Risen, "Los Alamos Scientist Admits Contacts with Chinese, US Says," *New York Times*, March 16, 1999, <http://www.nytimes.com/1999/03/16/world/los-alamos-scientist-admits-contacts-with-chinese-us-says.html>.
109. Risen and Gerth, "US Says Suspect Put Code on Bombs in Unsecure Files."
110. Purdy, "The Prosecution Unravels."
111. Risen and Gerth, "Breach at Los Alamos."
112. Purdy, "The Prosecution Unravels."
113. Risen and Gerth, "Breach at Los Alamos."
114. Johnston and Risen, "The Los Alamos Secrets Case."
115. Johnston, "Suspect in Loss of Nuclear Secrets Unlikely to Face Spying Charges."
116. Ibid.
117. Risen, "Los Alamos Scientist Admits Contacts with Chinese."
118. Ibid.
119. Johnston and Risen, "The Los Alamos Secrets Case."
120. Broad, "Files in Question in Los Alamos Case Were Reclassified."
121. Sterngold, "US to Reduce Case against Scientist to a Single Charge."
122. Purdy, "The Prosecution Unravels."
123. 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).

5 Jousting with Cuba over Radio Marti

By Rudolph Rousseau

Key Questions

- ▶ **How was Cuban President Fidel Castro likely to react to a US decision to initiate radio broadcasts from Florida into Cuba with Radio Marti?**
- ▶ **What could Castro do to prevent, mitigate, or delay the broadcasts?**
- ▶ **Was his strategy in dealing with the United States likely to be fundamentally proactive or reactive?**
- ▶ **What were the risks and benefits of initiating Radio Marti broadcasts for the Reagan administration?**

CASE NARRATIVE

A Modest Skirmish in a Global Confrontation

By the time US President Ronald Reagan came into office in 1981, the United States and Cuba had been in direct conflict for two decades. Over the years, Fidel Castro had used multiple measures to annoy the United States, including increasing interference with US commercial broadcasts. For example, despite Cuba's signing of the North American Radio Broadcasting (NARB) Agreement in 1950, Cuban interference on the AM band began to grow in the 1960s after Castro came to power; by the 1970s, it was a serious problem. In 1979, Cuba submitted an inventory to the International Telecommunications Union (ITU) that included plans for two radio stations transmitting 500 kilowatts (kW) of power—a volume ten times the limit permitted to any US radio station.¹

A core objective of President Reagan's national security strategy was to confront the Soviet Union and its allies globally on economic, political, and military battlefronts—both large and small. Cuba was one of the Soviet Union's allies. Radio Marti was a weapon on one of those fronts.

According to a State Department official serving on the Cuban desk at the time, "Breaking Cuba's domestic monopoly of information was an important element of the Reagan administration's plan to put Fidel Castro on the defensive. The collapse of the Soviet Union and its economic subsidies had already severely damaged the Cuban economy, resulting in an explosion of popular discontent. By 1980, that discontent had demonstrated that despite its

capacity to project power aboard, Cuba's internal social order was insecure.”²

The Reagan administration's rationale for establishing Radio Marti was to “provide news, commentary, and other information about the events in Cuba and elsewhere to promote the cause of freedom in Cuba.”³ The final phrase in that statement was a direct challenge to the Cuban regime. Although Radio Marti broadcasts would not pose the same level of threat to the Castro regime as the Bay of Pigs invasion, covert assassination plans, the tension of the Cuban Missile Crisis, or the long-standing US trade embargo, it would funnel uncontrolled information to the Cuban people.

As an element of President Reagan's political strategy, Radio Marti would also serve the interests of his Cuban American constituency in Florida. Reflecting these political sensitivities, the Reagan administration originally proposed that the station be operated by Radio Broadcasting to Cuba, Inc.—an independent, nonprofit corporation, incorporated in September 1981—and not under the Board for International Broadcasting, which was the parent organization of Radio Free Europe (RFE), Radio Liberty (RL), and the Voice of America (VOA).⁴

A Key Intelligence Question

As the Reagan administration developed its plans for Radio Marti and Congress considered the administration's legislative proposals to establish the news service, a key question was, “How will Cuba respond to the new radio service?” Fidel Castro's response, both publicly and privately, was unequivocal. He threatened to disrupt AM broadcasting throughout the United States if the Reagan administration began Radio Marti broadcasts to Cuba.⁵

If Castro carried out his threat, US broadcasters could suffer significant economic damage. Should Congress ignore the concerns of some key constituents that the launch of Radio Marti would threaten the interests of US broadcasters, truckers, and farmers? More important, from the president's perspective, the administration could be faced with the prospect of looking impotent in the face of Cuban retaliation. Should President Reagan cancel plans to launch Radio Marti to avoid any disruption of US domestic commercial radio broadcasts, or should he choose to mount a joint diplomatic and military response to deter Cuba from retaliating? Both of those options carried significant domestic political and foreign policy risk.

The Leaders' Policy and Personal Stakes

National security issues are often portrayed as somewhat abstract policy choices in which the national leaders engage on an intellectual and political level. The Radio Marti proposal was a traditional national security issue. However, it also struck personal chords with Ronald Reagan, Fidel Castro, and the Cuban American community. Personal stakes can sometimes affect traditional national security calculus.

President Reagan. Before Ronald Reagan was a politician or an actor, he was a radio announcer. Between 1933 and 1937 he was a sports broadcaster on WHO, a 50 kW clear channel station broadcasting on 1040 kilohertz (kHz) located in Des Moines, Iowa,⁶ with listeners across the Midwest. In August 1981, during technical discussions concerning radio interference, Cuba said it would move forward with plans for two 500 kW stations and broadcast on 1040 kHz—the frequency designated for both Radio Marti in Florida and WHO in Iowa.⁷

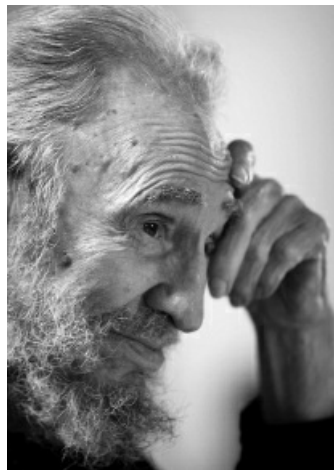
On 30 August 1982, a 150 kW Cuban transmission on 1040 kHz disrupted WHO

broadcasts.⁸ Fidel Castro's threat to retaliate against Radio Marti directly affected Ronald Reagan's radio alma mater.

President Castro. Fidel Castro, personally, and his government, generally, had been the target of US efforts to end his life and his regime since its inception in 1959. Operation Mongoose was one effort to overthrow the regime and likely had elements intended to assassinate Castro.⁹ The Bay of Pigs invasion in 1961 and the US economic embargo of Cuba in 1962 were others. Fidel Castro unquestionably perceived Radio Marti as another challenge to him personally and the success of his revolution.



Ronald Reagan, WHO Radio sports announcer.



Cuban President Fidel Castro.

The Cuban American Community. The Cuban American community in the United States was the principal advocate for Radio Marti.¹⁰ Many Cuban Americans had direct personal interest in the success of Radio Marti and the risks associated with initiating broadcasts. Many of the most prominent members of that community had fled Cuba after Castro came to power. A significant number had lost friends and relatives to revolutionary "justice," and most lost their wealth. In addition, Spanish-language radio broadcasters in south Florida had been affected by interference from Cuban stations for many years and risked additional economic damage if Castro carried out his threats to disrupt US stations in retaliation for Radio Marti's broadcasts.¹¹ During the 1980s,

the Cuban American community had a direct and personal stake in negotiations with Cuba that could increase their access to the island and their ability to secure permission for relatives to leave.¹²

Key US Stakeholders

The Reagan administration's proposal to broadcast Radio Marti's messages to Cuba and Fidel Castro's threats to disrupt US broadcasting in response affected the interests of several politically active and potent interests in the United States.¹³

- ▶ The **National Association of Broadcasters** (NAB) represented commercial broadcasters across the United States. NAB members were concerned about the potential for disruption of their programs and the economic losses that would follow. The NAB had an extensive lobbying arm in Washington with ready access to members of Congress.
- ▶ In contrast, **radio station broadcasters in south Florida**, who had been affected by interference from Cuban stations for many years, generally supported Radio Marti in solidarity with their Cuban American listeners.¹⁴
- ▶ **Agricultural interests** in the Midwest were concerned about the potential for disruption of programming important to farmers who needed reports providing agricultural information broadcast over the radio.
- ▶ **Truckers** who listened to clear channel radio programming during their overnight runs did not want their broadcasts disrupted.

Members of Congress reflected these concerns. The south Florida delegation actively supported the Radio Marti proposal, while midwestern members who represented broadcasters, farmers, and truckers were often skeptical.¹⁵ In 1982, the South Florida Association of Broadcasters urged the administration to build facilities to jam Cuban radio operations until Cuban interference ended.¹⁶

The Proposal

On 22 September 1981, President Reagan signed Executive Order 12323 to establish the Presidential Commission on Broadcasting to Cuba. The executive order "was accompanied by a statement expressing the administration's belief that breaking Havana's information monopoly would help the Cuban people judge the Cuban revolution on its true merits."¹⁷

The Executive Order stated that "the Commission shall develop a recommended plan for radio broadcasting intended for transmission to Cuba. The purpose of the plan shall be to promote open communication of information and ideas to Cuba and in particular broadcasting to the Cuban people of accurate information about Cuba."¹⁸

The commission, with strong representation from south Florida among its members, recommended establishing a new radio service for Cuba.¹⁹ On 2 February 1982, the Reagan administration introduced its proposed legislation to establish Radio Marti.²⁰ The House moved quickly to establish Radio Marti as a service. H.R. 5427 was approved by the House on 10 August 1982. Radio Marti was authorized to broadcast on 1040 kHz with 50 kW of power. It would broadcast on the same frequency as WHO but would not interfere with its signal. The

legislation also included a congressional provision urging the president to “seek a practical political and technical solution” to the threats of Cuban interference.²¹

Castro Ups the Ante

One month before President Reagan formally announced the proposal to establish the Presidential Commission on Broadcasting to Cuba, the Cubans announced their intention to shift the frequencies of its 500 kW stations to 1040 kHz and 1160 kHz. Those frequencies represented a threat to clear channel commercial broadcasts in the United States.

With the Senate Committee on Foreign Relations planning to consider the legislation, the administration appeared to be on a fast track to begin broadcasts to Cuba over Radio Marti. Then Fidel Castro placed a radio wave roadblock in the administration’s path. On 30 August 1982, Cuban broadcasts disrupted WHO on 1040 kHz in Des Moines, Iowa; KSL on 1160 kHz in Salt Lake City, Utah; and several other stations across the United States.²² The FCC had assessed that at full power Cuba’s two 500 kW transmitters could be heard in Alaska and Hawaii.²³ (See Figure 5.1.)

Farmers and truckers heard the Cuban broadcasts firsthand. The NAB, citing the broadcasts, became particularly active in advocating that Congress delay implementation.²⁴ Members of the Senate Committee on Foreign Relations, listening to their constituents, began to consider how best to respond.

The Senate Committee modified the Radio Marti legislation and reported it out of committee on 9 September, but, more important, on 21 December 1982 the Senate declined, by voice vote, to take up the legislation. That defeat reflected the NAB’s lobbying and senators’ concerns about the potential for damage to their constituencies.²⁵

Figure 5.1 ▶ Cuban Capabilities to Disrupt US Radio Broadcasting



Source: Adriana Gonzalez, Pherson Associates, LLC.

Radio Marti legislation was revived at the beginning of the 98th Congress. House Foreign Affairs Committee Chairman Dante Fascell, a longtime Democratic congressman with a Miami

district, presided over the hearings and eventual passage of the bill by his committee.²⁶ The south Florida constituency had won a round. However, the NAB's friends on the House Energy and Commerce Committee reported out another bill changing Radio Marti from a surrogate Cuban station to a more standard, objective model under the Voice of America.²⁷ The same political dynamics that had led to the bill's defeat in the Senate at the end of the previous Congress were reflected in this House stalemate.

The administration attempted to respond to the NAB's concerns by engaging the Cubans in negotiations on radio interference in August 1983. Industry representatives were part of the US delegation. These talks produced no agreement—the Cubans still opposed Radio Marti, and the Reagan administration supported it. The NAB continued to lobby against the legislation.²⁸

The bill's prospects in the Senate were subject to the same political dynamics leading to stalemate in the House. The bill had been reported from the Foreign Relations Committee, but Sen. Lowell Weicker, a Republican senator from Connecticut, was preventing it from moving forward. A Florida Republican, Paula Hawkins, and a Nebraska Democrat, Edward Zorinsky, convinced Weicker to accept a compromise on the legislation. They agreed to shift Radio Marti to the supervision and standards of the Voice of America and to change its frequency to 1180 kHz in order to remove the threat to WHO on 1040 kHz. The legislation was adopted by voice vote in the Senate on 13 September 1983.²⁹

At this point, the Reagan administration was on the verge of having a Radio Marti, but not the Radio Marti that it originally proposed. The House was poised to pass the Senate bill with the Weicker compromise as its key provision. Then, Undersecretary of Secretary of State Lawrence Eagleburger convinced the floor manager of the bill, Chairman Dante Fascell, to make a statement prior to the bill's passage that Radio Marti would be a surrogate home broadcasting service for Cuba.³⁰ That legislative history would enable the administration to use Radio Marti as it intended from the beginning. Congress passed the bill and sent it to the president for his signature on 29 September.

President Reagan signed the bill into law on 4 October 1983.³¹ Through the nearly three years of administration and congressional consideration of Radio Marti, Cuban opposition, intentions, and capabilities had been critical factors. The Cubans had played many of the strings of the American political instrument. However, at the end of the day, Radio Marti was established with a mandate to serve as a surrogate broadcaster to Cuba.

Two Questions for the US Administration

Authorization to establish Radio Marti, however, did not end the game. The administration still needed to determine the content of the broadcasts and the details of setting up the station, hire a staff, and decide what type of content to include in the programming. Would Radio Marti broadcasts actively challenge the Castro regime, or would they more closely parallel Voice of America broadcasts? The Cubans had additional opportunities to influence those decisions. The field of play had now shifted from the US Congress to the executive branch.

The president had been clear from the beginning of his administration that he wanted Radio Marti to provide alternative information to the Cuban people.³² The key questions on his desk now were

- ▶ How would Cuba respond to Radio Marti's broadcasts?
- ▶ How could the United States influence Cuba's response?

The first was an analytic question; the second a policy question.

How Would Cuba Respond? By 1983, the principal elements of the analytic problem were well established:



Radio Martí's antennae field.

- ▶ **Open and Clandestine Sources.** Cuba had expressed its opposition to the establishment of Radio Martí clearly and consistently. Cuban opposition had been conveyed in speeches by Fidel Castro and in many other official sources. In addition, as Kenneth Skoug Jr., Cuban desk officer at the US State Department, observed, the United States had clandestine sources reporting that Cuba would take various actions to demonstrate its opposition to the broadcasts.³³
- ▶ **Capabilities.** Cuba had amply demonstrated its capability to disrupt US AM broadcasting across the country. Furthermore, it had done so in response to the Radio Martí proposal.
- ▶ **Compromise.** The Cubans had engaged in radio interference negotiations and had indicated a willingness to accept Radio Martí as another outlet of the Voice of America, largely because of the significant difference in content that would imply.
- ▶ **Motive.** Cuba carefully controlled the regime's message to the Cuban people. That effort was a critical element in its governing structure. Alternative information, particularly in times of unrest, could be a threat to the government message and program. Castro probably feared that Radio Martí could be used to help articulate grievances against the regime and to stimulate, either indirectly or directly, organized discontent. The Cubans' motive to prevent Radio Martí from broadcasting or influencing the content of its broadcasts was clear.

Cuba had been successful in using a combination of its disruptive broadcasting capabilities and its opposition to Radio Martí to convince significant US broadcasting, trucking, and farming interests—and the US senators who represented them—that Radio Martí, as proposed by the administration, was not worth the risk of economic damage.

Analysis of Castro's intentions was derived fundamentally from information from open and clandestine sources, the evaluation of Cuban capabilities to disrupt US broadcasting, and Cuba's demonstrated willingness to do so. Analysts had little doubt that Castro *could* respond; the principal question for analysts at the time was *how* he would respond, and with what potential repercussions for the United States. For the administration, that was all the difference in the world.

Castro had been playing the great game with the United States for two decades. At times, during the Cuban Missile Crisis, for example, he had demonstrated a willingness to take aggressive and extremely risky action. During the 1970s and early 1980s, he had sent Cuban troops to Africa, Central America, and Latin America to support revolutions and was directly confronted by the United States in the process. He had lived with the impact of the US embargo at great cost to the Cuban people. That track record indicated a past willingness to engage the United States directly, but it did not establish what he would do in the case of Radio Marti.

The most dispositive data concerning intentions came from reporting on the private statements of intent by Castro himself. As widely reported, Cuban Dirección General de Inteligencia (DGI) defector Major Florentine Aspillaga established that the United States received reporting from numerous clandestine agents in Cuba. Reporting from some of those agents likely provided insights about Castro's intentions to respond to Radio Marti.³⁴ In the words of State Department Desk Officer Skoug, "a very skillful use of intelligence channels would continue to hold Washington's attention. US decisions about Radio Marti would be influenced by the threat of Cuban radio interference and its impact on the US broadcasting industry."³⁵

How Could Washington Influence Castro's Behavior? The Reagan administration estimated that Castro's response to Radio Marti could be influenced by its own plans to respond to any radio interference from Cuba. The Reagan administration needed to develop a means to either persuade Castro that the costs of disrupting US radio broadcasts were too high or, if he engaged in disruption, to convince him to stop.

Developing US countermeasures to Cuban radio interference had been included as a requirement in the original House-passed legislation, H.R. 5427.³⁶ In addition, on 10 September 1982, in the wake of Cuba's disruption of US broadcasters, Secretary of State George Shultz asked for a briefing on "what countermeasures were available in the event disruptions continued."³⁷ The *New York Times* reported that, on 7 May 1983, senior administration officials had told commercial broadcasters that a list of forty options was under consideration, including bombing antennas in Cuba if Castro jammed US radio stations.³⁸

Discussions about countermeasures continued through the fall of 1983. According to Skoug, at a 19 December meeting at the White House Situation Room, he "mentioned the need to have appropriate reprisals ready if Cuban reaction materialized as we feared."³⁹ Skoug also wrote, "In separate conversations on April 5, National Security Council staffers Constantine Menges and John Lenczowski expressed to [State Department Official] John Ferch and me a preference for military countermeasures if Cuba disrupted radio broadcasting in the United States."⁴⁰

Skoug's recollections and the *New York Times* report provide an outline of the Reagan administration's retaliatory planning if Cuba responded to Radio Marti's startup by interfering with US commercial radio stations. The administration was not only developing plans, but by leaking their existence to the *New York Times* through a "senior official," those plans were

indirectly communicated to Cuba. As Cuba's 1982 demonstration of the reach of its transmitters raised the stakes for the United States, the administration's countermeasure plans upped the ante for Castro.

Tensions remained high throughout the next year. In a March 1984 interview published in the *Washington Post*, Cuban Vice President Carlos Rafael Rodriguez labeled Radio Marti as "another US aggression" and indicated that "Cuban counter-broadcasting would be in proportion to the tone of Radio Marti programming."⁴¹

What Washington would decide to do, however, remained an open question. As President Reagan noted in his personal diary later that year:

We are ready to go with "Radio Marti" our station broadcasting truth to Cuba—part of our Information Program. Cuba, however, threatens retaliation; not just jamming our program but jamming Am. radio stations all the way to the Mid-west. They are actually completing the transmitters to do this. We can join [sic] all of theirs but at great cost & only after several months. It will take time to set up a system. If we retreat we lose face which can hurt us in all of Latin Am. If we go forward we could knock many of our commercial stations off the air. What to do? Right now I don't know.⁴²

A Radio War with Cuba?

US analysts charged with estimating how Cuba would respond to the launch of Radio Marti had an unusually rich collection of data with which to work. The core facts were well established from multiple sources. Cuba had:

- ▶ Stated its opposition to Radio Marti
- ▶ Publicly threatened to retaliate if Radio Marti began broadcasting as a surrogate radio to Cuban audiences
- ▶ Declared its possession of 500 kW transmitters to the International Telecommunication Union (ITU)
- ▶ Demonstrated its capacity to use those transmitters to disrupt US commercial radio broadcasts

Analysts were also aware that general plans for aggressive countermeasures had been communicated to the Cubans. The specific operational plans were confined to a small group of White House, Intelligence Community, and Department of Defense officials. Intelligence analysts responsible for estimating Cuba's response had also been directly involved in developing countermeasures.

The central analytic problem was to estimate what Castro would do. Would he:

- ▶ Carry out his threats to retaliate and interfere with US radio broadcasts and ignore the prospect of US countermeasures?
- ▶ Retaliate by taking action relating to some other aspect of US–Cuban relations?
- ▶ Choose not to retaliate but only to jam incoming broadcasts, satisfied that his aggressive posture had delayed Radio Marti for more than three years and modified its content sufficiently by forcing Washington to place it under the authority of the VOA?

RECOMMENDED READINGS

- Latell, Brian. *Castro's Secrets: The CIA and Cuba's Intelligence Machine*. New York: Palgrave McMillan–St. Martin's Press, 2013.
- Skoug, Kenneth N., Jr. *The United States and Cuba under Reagan and Shultz: A Foreign Service Officer Reports*. Westport, CT: Praeger, 1996.
- Walsh, Daniel C. *An Air War with Cuba: The United States Radio Campaign against Castro*. Jefferson, NC: McFarland & Company, 2012.

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

JOUSTING WITH CUBA OVER RADIO MARTI

Structured Analytic Techniques in Action

The US government jousted with Cuba for four years over radio broadcasts to Cuba from Florida. Cuban President 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.

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.

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.

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?

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?

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 the targets of deception, such as the timing of reporting, the bona fides of a source, or when believing what a source says would 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: Assess whether a good case can be made to employ Deception Detection techniques using Table 5.2 as your guide. If a case can be made that Cuba has a motive to deceive, state this as a hypothesis to be proved or disproved.

Table 5.2 ▶ When to Use Deception Detection

Analysts should be concerned about the possibility of deception when:
The potential deceiver has a history of conducting deception.
Key information is received at a critical time, i.e., when either the recipient or the potential deceiver has a great deal to gain or to lose.
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 the new information would cause the Intelligence Community, the US government, or the client to expend or divert significant resources.
The potential deceiver may have a feedback channel that illuminates whether and how the deceptive information is being processed, and to what effect.

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 as your guide.

Table 5.3 ▶ Deception Detection Templates	
Motive, Opportunity, and Means (MOM)	
Motive: What are the goals and motives of the potential deceiver?	
Channels: What means are available to the potential deceiver to feed information to us?	
Risks: What consequences would the adversary suffer if such a deception were revealed?	
Costs: Would the potential deceiver need to sacrifice sensitive information to establish the credibility of the deception channel?	
Feedback: Does the potential deceiver have a feedback mechanism to monitor the impact of the deception operation?	
Past Opposition Practices (POP)	
Does the adversary have a history of engaging in deception?	
Does the current circumstance fit the pattern of past deceptions?	
If not, are there other historical precedents?	
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?	
What is the basis for judging the source to be reliable?	
Does the source have direct access or only indirect access to the information?	
How good is the source's track record of reporting?	
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?	

Evaluation of Evidence (EVE)	
How accurate is the source's reporting? Has the whole chain of evidence, including translations, been checked?	
Does the critical evidence check out? Remember, the subsource can be more critical than the source.	
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)?	
Do other sources of information provide corroborating evidence?	

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 expose any embedded assumptions or critical gaps that need to be examined more critically?

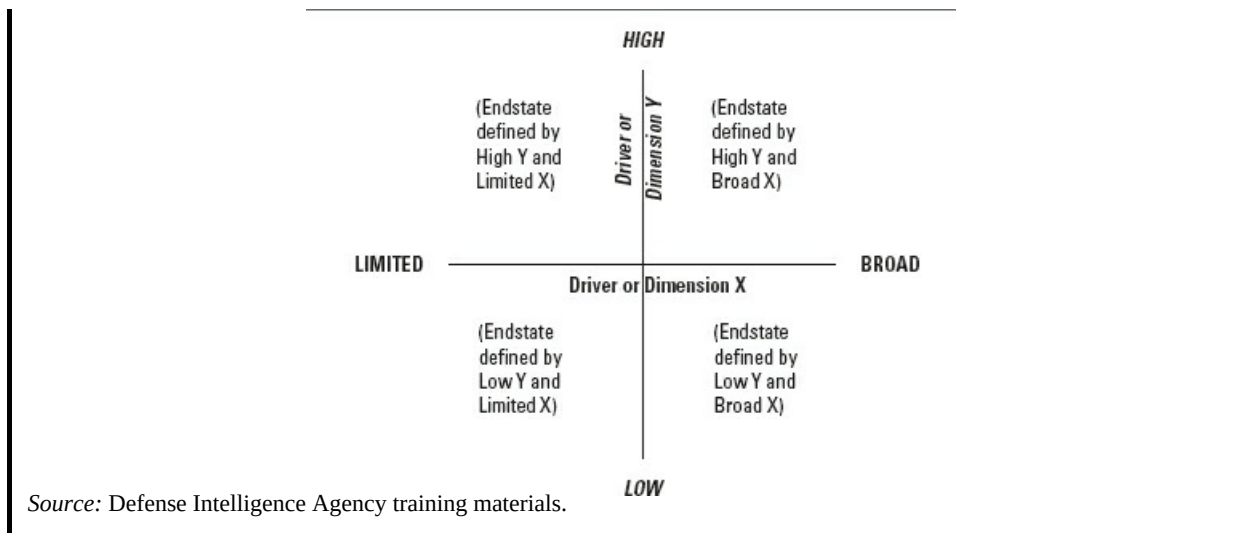
Technique 3: Quadrant Hypothesis Generation

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 GeneratorTM. The Multiple Hypotheses GeneratorTM 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.⁴³

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.

Figure 5.2 ▸ Quadrant Hypothesis Generation Template



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 Martí 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.
- STEP 2:** Construct a 2×2 matrix using the two drivers or primary dimensions of the issue (see Figure 5.2).
- 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.
- 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.

The following two steps 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 comprehensive? Did you generate more than one hypothesis or endstate for any of the quadrants?

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 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 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.
- 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 consistent, consistent, highly inconsistent, inconsistent, neutral, or not applicable vis-à-vis the hypothesis?” (The Te@mACH® software does not include the “neutral” category.)
- 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?
- 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.
- 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.
- STEP 7:** Report the conclusions by considering the relative likelihood of all the hypotheses.
- STEP 8:** Identify indicators or milestones for future observation.

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?

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. Ibid., 17.
3. Radio Broadcasting to Cuba Act, PL 98-111.
4. Joel M. Woldman, *Radio Marti Issue Brief*, no. IB83105 (Washington, DC: Library of Congress Congressional Research Service), 2.
5. For an extended discussion of the internal debate see Skoug, *The United States and Cuba under Reagan and Shultz*.
6. George F. Davison Jr., "Ronald Reagan: A Salute to the Fortieth President of the United States and Former WHO Sports Director," DesMoinesBroadcasting.com.
7. Skoug, *The United States and Cuba under Reagan and Shultz*, 17.
8. David Shribman, "Cuba Disrupts U.S. Radio as Distant as Des Moines," *New York Times*, September 1, 1982, Sec. A., 11, and *New York Times*, September 3, 1982, Sec. B, 6.
9. Foreign Relations of the United States 1961–1963, Vol. 10, and Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities Alleged Assassination Plots Involving Foreign Leaders, 94th Congress, 1st session, November 1975. Cited in Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Addison-Wesley Educational Publishers, 1999).
10. Reginald Stuart, "Miami's Community of Republican Cubans Awaits Reagan with Excitement," *New York Times*, May 20, 1983, Sec. A, 15.
11. Skoug, *The United States and Cuba under Reagan and Shultz*, 16.
12. Joseph B. Treaster, "Radio Marti Goes on Air and Cuba Retaliates by Ending Pact," *New York Times*, August 20, 1985, Sec. A, 10.
13. Woldman, *Radio Marti*, 9.
14. Skoug, *The United States and Cuba under Reagan and Shultz*, 18.
15. Sen. Paula Hawkins (R-FL) sponsored the legislation in the Senate and Rep. Dante Fascell (D-FL) in the House. Sen. Edward Zorinski (D-NE) and Timothy Wirth (D-CO) were the principal opponents of the legislation. See Judith Miller, "Quarrel in Senate over Radio Marti," *New York Times*, August 2, 1982, Sec. 1, 3.
16. Skoug, *The United States and Cuba under Reagan and Shultz*, 19.
17. Statement by Assistant to the President for National Security Affairs Richard V. Allen Concerning Radio Broadcasting to Cuba, September 23, 1981.
18. Executive Order 12323.
19. Skoug, *The United States and Cuba under Reagan and Shultz*, 18.
20. Woldman, *Radio Marti*, 9.
21. Skoug, *The United States and Cuba under Reagan and Shultz*, 19.
22. Shribman, "Cuba Disrupts U.S. Radio."
23. Skoug, *The United States and Cuba under Reagan and Shultz*, 18.
24. Ernest Holsendolph, "U.S. Lists 'Options' on Cuban Jamming," *New York Times*, May 7, 1983, Sec. 1, 5.
25. Skoug, *The United States and Cuba under Reagan and Shultz*, 19.
26. Ibid., 20.
27. Ibid.
28. Ibid.
29. Susan B. Epstein and Mark P. Sullivan, *Cuba: Background and Issues through 1994*, Congressional Research Service, 2.
30. Ibid.
31. Ibid.
32. Skoug, *The United States and Cuba under Reagan and Shultz*, 17.
33. Ibid., 23.
34. Ibid. 23; 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," *Washington Post*, August 12, 1987.
35. Skoug, *The United States and Cuba under Reagan and Shultz*, 23.
36. Ibid., 19.
37. Ibid.
38. Holsendolph, "U.S. Lists 'Options.' "
39. Skoug, *The United States and Cuba under Reagan and Shultz*, 23.
40. Ibid., 56.
41. Woldman, *Radio Marti*, 9. In his article, Woldman provides the quotation as taken from the *Washington Post*, March 14, 1984.
42. Daniel C. Walsh, *An Air War with Cuba: The United States Radio Campaign against Castro* (Jefferson, NC: McFarland

& Company, 2012), 91.

43. For more information on the Multiple Hypotheses GeneratorTM, go to <http://www.globalytica.com>.

6 The Road to Tarin Kowt

Key Questions

- ▶ What are the strategic, operational, and tactical goals of the mission?
- ▶ What could threaten these goals?
- ▶ How can the United States improve the odds of achieving its goals in the region?

CASE NARRATIVE

The route from Kandahar to Tarin Kowt rises out of the dusty and largely uninhabited Iranian plateau south of Kandahar and continues into the rocky foothills of the Hindu Kush, the central mountain range in Afghanistan. The topography and weather are inhospitable, if not brutal, and the dry and dusty region—often obscured by sudden *khahbad* (dust winds)—becomes gravelly and boulder strewn as the foothills grow more mountainous near Tarin Kowt.

In 2004, the 117-kilometer (km) route between these two provincial capitals was not much more than a dusty path through a known Taliban stronghold. International donor conferences had identified building road infrastructure as a critical element in efforts to stabilize, modernize, and democratize Afghanistan, and the United States had taken on the challenge of building a modern road along this centuries-old route. By April 2005, the US Army had completed 46.5 kilometers of road over a period of nine months.¹ With the road about a third complete and Afghanistan's first parliamentary elections since the overthrow of the Taliban announced for 18 September, the Army considered embarking on a highly accelerated schedule to complete the road in time for the election. Lt. Gen. Karl Eikenberry, who assumed command of the US Combined Forces Command Afghanistan in early May 2005, assessed the stakes involved in the project succinctly: "Wherever the road ends, that's where the Taliban starts."²

Completing another 70.5 kilometers of road in a mere five months not only would be a formidable engineering and logistical challenge but also would raise serious questions about mission security and engagement with the local population. The United States faced an important decision point that had major strategic, operational, and tactical implications. A sound course of action would require a thorough analysis of the operating environment, anticipated enemy response, and the potential impact on broader US goals for Afghanistan.



By the spring of 2005, US Army Engineers had completed 46.5 kilometers of road between Kandahar City in Kandahar Province and Tarin Kowt in Uruzgan Province.

The Pashtun Way

The road from Kandahar to Tarin Kowt traverses a region that is heavily Pashtun—a predominantly Sunni Muslim group of some 40 million people concentrated in southern and eastern Afghanistan and neighboring parts of Pakistan. The Pashtun are the world’s largest ethnicity lacking an independent state. The mostly agrarian society practices a stringent code of Pashtunwali—or “way of the Pashtun”—that provides a different set of social norms than those of central government or traditional tribal rule (see Table 6.1). Abjuring hierarchal leadership and formal courts and laws, Pashtunwali is built on complex traditions of individual independence, collective conflict resolution mechanisms, and shared honor codes that guide all aspects of Pashtun life. The main tenets of Pashtunwali stress aspects of hospitality, bravery, and justice, which means that “honor and hospitality, hostility and ambush, are paired in the Afghan mind.”³

In Pashtun society, no adult male has the authority to tell another man what to do. Unlike the neighboring Baluchi ethnic group, whose *sardars* have many of the powers of a traditional tribal chief, “any sort of external direction is not merely abhorrent to Pashtuns, but lies beyond their mental compass.”⁴ In the absence of traditional tribal leadership, informal patronage networks have come to determine politics in Afghanistan’s provincial regions. Whereas Pashtunwali and Islam are time honored, patronage networks are temporary constructs. Local patrons—*khans*, or warlords—are not elected and do not hold any formal office. A warlord’s power is based on his ability “to distribute resources to make a convincing case for his leadership.”⁵ As a result, the dynamics are unique to the network, reflecting shifts in local power relationships.⁶

Although all Pashtuns practice Pashtunwali, there are significant differences between those farming at lower elevations, who have historically been susceptible to taxation, and those living in the hills, who pride themselves on their social equality and freedom from any authority. For rural Pashtuns in the former group, day-to-day life centers around farming and subsistence living.⁷ Their homes are principally made of mud, and they are sparsely decorated with essential cooking implements and mats for sleeping. They must serve as their own irrigation specialists,

construction experts, veterinarians, and security forces. Their survival depends on their ability to farm the land successfully, and they guard their land closely. Village Pashtuns view any outsider with great skepticism, which is shaped by a shared memory of battles against infidel invaders, but Pashtunwali obligates them to extend hospitality and temporary protection to all guests who seek it, even those they regard as enemies.⁸ As a result, the village defends its ways by building a metaphorical “mud curtain”—a cultural defense mechanism that Pashtuns have developed over centuries of interactions with invaders, well-meaning central governments, and foreign “modernizers.”⁹ They quickly agree with outsiders and accept their projects, but only because the more quickly they do so, the sooner the outsiders will leave and the villagers can return to their “old, group-reinforcing patterns.”¹⁰

Table 6.1 ▶ Tenets of Pashtunwali

A Pashtun derives honor from practicing the following tenets of Pashtunwali:

To avenge blood.

To fight to the death for a person who has taken refuge with me no matter what his lineage.

To defend to the last any property entrusted to me.

To be hospitable and provide for the safety of the person and property of guests.

To refrain from killing a woman, a Hindu, a minstrel, or a boy not yet circumcised.

To pardon an offense on the intercession of a woman of the offender's lineage, a *sayyid* [Islamic chief], or a *mullah* [Islamic cleric].

To punish all adulterers to the death.

To refrain from killing a man who has entered a mosque or the shrine of a holy man so long as he remains within its precincts; also to spare a man in battle who begs for quarter.

Source: Louis Dupree, *Afghanistan* (Princeton, NJ: Princeton University Press, 1980), 126.



Kandahar and Uruzgan provinces are largely agrarian outside the major cities. Predominantly ethnic Pashtun inhabitants of the region practice a strict code of Pashtunwali that governs all aspects of daily life. Farmers must serve as their own irrigation specialists in a region that can see both drought and flood in a single season.

For Pashtun hill society, “central government and externally imposed order are not simply anathema but the antithesis of what is good,”¹¹ and it passionately resists them. Insurgency in Afghanistan has typically arisen from this hill culture, driven less by economic deprivation than by deeply held cultural and religious norms. Moreover, the Pashtunwali code makes the attrition of Pashtun insurgents nearly impossible; the death in battle of a Pashtun guerrilla invokes an obligation of revenge among all his male relatives, making the killing of a guerrilla an act of insurgent multiplication, not subtraction. The Soviets learned this lesson; they killed nearly a million Pashtuns but only increased the number of opposition fighters by the end of the war.¹² It was from this Pashtun hill culture that the Taliban arose.

Box 6.1 SOVIET LESSONS LEARNED

From 1979 until 1989, the Soviet Union fought a grueling war in Afghanistan. The Soviets invaded the country ostensibly to support the pro-Soviet communist leadership and to “stabilize the country.”ⁱ They expected a quick and successful military operation, but the plan backfired in the face of significant resistance from US- and Pakistani-backed mujahidin, the Kabul regime’s weak capacity for governance, and Afghanistan’s unforgiving geography.ⁱⁱ

Soon after the invasion, the war “devolved into a fight for the control of the limited lines of communication, [specifically] the road network which connected the cities of Afghanistan with each other and to Pakistan and the Soviet Union.”ⁱⁱⁱ Despite the Soviets’ massive influx of troops, which at the height of the war topped 100,000, the mujahidin became skilled at conducting ambushes on Afghanistan’s road network. These disrupted Soviet supply lines and contributed to heavy personnel and equipment losses, including “11,389 trucks, 1,314 armored personnel carriers, 147 tanks, [and] 433 artillery pieces.”^{iv} The mujahidin’s weapons of choice against the convoys included “antitank, antipersonnel, and dummy mines, as well as controlled mines and improvised explosive charges.”^v

In the face of repeated losses, the Soviets eventually learned that for a convoy escort to have a chance at success, it needed dedicated security units with a rapid reaction capability; armored vehicles, armed with sufficient firepower and forces ready for ground combat; route reconnaissance units reinforced with ground forces to secure flanks and identify ambush sites; planned air and artillery support; engineers embedded with the convoys for route clearance; and operational security underpinned by unpredictability of movement.^{vi}

Despite marginal improvements in convoy security, when Mikhail Gorbachev became general secretary of the Communist Party of the Soviet Union in 1985, it was becoming increasingly clear that victory was impossible, and Gorbachev soon made ending the conflict a top priority. The result of the invasion, he later said, was “the opposite of what we had intended: even greater instability, a war with thousands of victims, and dangerous consequences for our own country.... The greatest mistake was failing to understand Afghanistan’s complexity—its patchwork of ethnic groups, clans and tribes, its unique traditions and minimal governance.”^{vii} By the time of the Soviet withdrawal, the war had officially claimed 15,000 Soviet and 1 million Afghan lives, although many experts believe that the conflict took many more lives than officially reported.

-
- i. Mikhail Gorbachev, "Soviet Lessons from Afghanistan," *New York Times*, February 4, 2010, <http://www.nytimes.com/2010/02/05/opinion/05iht-edgorbachev.html>.
 - ii. Ibid.
 - iii. Lester W. Grau, "Convoy Escort in Guerrilla Country: The Soviet Experience," *Military Police* (Winter 1995), <http://fmso.leavenworth.army.mil/documents/convoy/convoy.htm>.
 - iv. Ibid.
 - v. Graham H. Turbiville Jr., "Soviet Combat Engineers in Afghanistan: Old Lessons and Future Wars," *Military Engineer* 80, no. 524 (1988); "Mine Clearing and Movement Support," <http://fmso.leavenworth.army.mil/documents/sovcombat/sovcombat.htm>.
 - vi. Ibid.
 - vii. Gorbachev, "Soviet Lessons from Afghanistan."

"Land of the Unruly"

Afghanistan's Amir Abdur Rahman Khan (1840 or 1844–1901) famously called his country the "Land of the Unruly." This was certainly an apt description of the Kandahar region in 2004, when it was the hotbed of a formidable Taliban insurgency focused on destroying the central Afghan administration and driving out the US and NATO (North Atlantic Treaty Organization) presence.¹³ The Taliban had its origins in the brutal civil war among rival warlords and their militias that followed the Soviet withdrawal in 1989, which devastated the country and destroyed what was left of the traditional tribal leadership system. With funding from Saudi Arabia and support from Pakistan's Inter-Services Intelligence Directorate (ISID), the Taliban emerged from *madrassas* (Islamic religious schools) near Ghazni and Kandahar in Afghanistan and in Pakistan's North-West Frontier Province (NWFP) and federally administered tribal area (FATA). It arrived on the Afghan scene in 1994 with little warning and vowed to install a traditional Islamic government and end the fighting among rival militias. With massive covert assistance from Pakistan, it overthrew the largely Tajik (and northern) regime in Kabul, capturing the capital in September 1996, in part by using "stunningly effective use of the roadways . . . to move forces faster and strike quicker."¹⁴ War-weary Afghans initially welcomed the Taliban, but Afghanistan soon became a training ground for Islamic activists and other radicals from the Middle East and around Asia. The country's optimism turned to fear as the Taliban introduced a stringent interpretation of Islamic law, banned women from work, and introduced such punishments as death by stoning and amputations.¹⁵

By the time the United States drove the Taliban from Kabul in late 2001, the Taliban's popularity in the country had waned considerably, but by most accounts it retained significant support in Kandahar and other parts of the Pashtun belt (see Map 6.1). This support was particularly strong among the Taliban's core of Ghilzai Pashtuns, longtime rivals of the nationalist and more moderate Durrani Pashtuns.¹⁶ Afghan President Hamid Karzai is a Durrani Pashtun. Support for the Taliban was high among the rural Pashtun population, and ethnic Pashtuns comprised a large percentage of the Taliban ranks; to extend its control, the Taliban played on the people's distrust of the cities, frustration with government corruption that disrupts basic services, and fear of foreigners.¹⁷ By 2004, the Taliban had regrouped and refocused its efforts on utilizing guerrilla warfare to rid Afghanistan of all US and NATO military forces. The Taliban's resurgence paralleled the Karzai government's struggles to establish a firm and legitimate foundation. The Kabul government was plagued by a weak capacity for governance,

inexperience, corruption, and an almost complete lack of presence in rural areas outside of the provincial capitals. US and NATO forces were able to do little to provide long-term security for those communities where the Taliban contested the power of village elders and warlords through coercion, intimidation, and assassination.¹⁸

Inroads with the People

The Soviet Union and the United States built most of Afghanistan's asphalt road infrastructure in the late 1950s and early 1960s as part of their foreign aid initiatives. Soviet and US aid supported the first two of Afghanistan's Five-Year Plans, which emphasized the creation of transportation and telecommunications infrastructure as means of improving the central government's connections with the people and its efforts to build a nation.¹⁹ During this period, foreign aid poured into Afghanistan and resulted in "one of the better road systems in Central Asia."²⁰ The aid built most of the existing portions of the Ring Road, which connects several of the provincial capitals to Kabul, and resulted in the famous Salang Tunnel that cuts directly through the Hindu Kush, a subrange of the Himalayas between central Afghanistan and northern Pakistan.

But by 2001, after decades of war and neglect, Afghanistan's roads were in disrepair, if not sharp decline. Only 16 percent of Afghanistan's roads were paved, and key communications and commerce links between many of Afghanistan's provincial capitals did not exist.²¹ To address this problem, the government of Afghanistan and international donors agreed in 2003 on a building and repair program for the country's road network, including completion of the Ring Road and construction of radial spokes from the ring to Afghanistan's outer provinces, in order to "spur economic development, promote governance, and improve security."²² The donors pledged billions of dollars to build Afghanistan's road infrastructure, and as of 2004, many international partners had begun construction on various roads. Leading the effort for the United States was the US Agency for International Development (USAID), along with the Department of Defense. In some cases, USAID paid contractors to build entire roads and, in other cases, to provide the finishing work—mostly paving—that USAID or the US Army could not complete themselves.

Map 6.1 ► Pashtun Tribal Areas and Insurgent Strongholds



As of 2005, the area between Kandahar City and Tarin Kowt was an insurgent stronghold.

Source: Pashtun Tribal Areas and Key Insurgent Strongholds, 2006, Figure 1, 77, in “Understanding the Taliban and Insurgency in Afghanistan,” <http://www.nps.edu/programs/ccs/docs/pubs/understanding%20the%20taliban%20and%20insurg> Reproduced with permission from Thomas H. Johnson and M. Chris Mason.

One of the complicating factors in the road construction initiative was that Afghanistan’s government, although ostensibly committed to upgrading roads, lacked clear legal delineation of roles and responsibilities among its various ministries and other organizations for managing and overseeing this work (see Table 6.2). As a result, there were redundancies in some areas—fee collecting, for example—and vacuums in others, such as maintenance.²³ Furthermore, the Afghan government faced “significant human and financial constraints” that limited its ability to develop and carry out a plan to maintain the roads.²⁴ Ensuring road security was another complicating factor, given the lack of effective state oversight. The roads were simultaneously an important part of the international community’s efforts to stabilize the country, the central government’s efforts to deliver services to and cultivate relations with the people, and the Taliban’s efforts to undo government ties with the people.²⁵

Task Force Pacemaker

Building a road through rough terrain is difficult enough, but building a road in a war zone presents unique and dangerous challenges. The Department of Defense funded the road project via the Commanders’ Emergency Relief Fund and tasked the US Army Corp of Engineers (USACE) with the project.²⁶ Between July 2004 and February 2005, the 528th Engineer Battalion of the Louisiana National Guard completed 46.5 km of the road from Kandahar City heading north toward Tarin Kowt. In March 2005, the 528th Engineers returned home, and the 864th Engineer Battalion from Fort Lewis, Washington, was poised to complete the road.

USACE has a long history of combat and reconstruction operations, and as a result, the 864th was equipped with an abundance of earth-moving heavy equipment, such as bulldozers, graders, and dump trucks; construction personnel, from land surveyors to construction designers and

planners; additional combat engineers trained to clear minefields and find hidden improvised explosive devices (IEDs); and additional maintenance personnel and repair assets to assist with the vehicles and equipment. The 864th would be operating in the most demanding of environments: at high altitude under a desert sun and working with fine, sticky, clay-based sand. This conglomeration of Army engineer units became known as Task Force Pacemaker.²⁷

Table 6.2 ► Afghan Ministries with Responsibilities for Roads, 2004–2005

Ministry	Road-Related Function
Public Works	Manages construction and maintenance for regional and national highways and most provincial roads
Rural Rehabilitation and Development	Manages construction of rural infrastructure, including rural roads and some provincial roads
Transportation and Civil Aviation	Inspects and issues commercial transit permits and collects fees from all domestic and international commercial vehicles
Finance	Collects road tolls on major highways
Interior	Manages registration and collection of fees for commercial and private vehicles, safety inspections, and traffic control
Commerce	Collects transit fees and can also charge a penalty for loads in excess of authorized limits
Foreign Affairs	Issues transit permits to foreign commercial vehicles entering and exiting Afghanistan
Economy	Conducts baseline studies for infrastructure projects. Its donor-supported unit currently is also responsible for all government procurement of goods and services, including road maintenance costing over \$200,000
Afghanistan Security Force	Responsible for ensuring security of roads but often delegates this role to local police and contract militia

Source: This chart is largely taken from the USAID information cited in the US Government Accountability Office report *Afghanistan Reconstruction Progress Made in Constructing Roads, but Assessments for Determining Impact and a Sustainable Maintenance Program Are Needed*, GAO-08-689, July 2008, 34, with the exception of the additional line on the Afghanistan National Security Force.

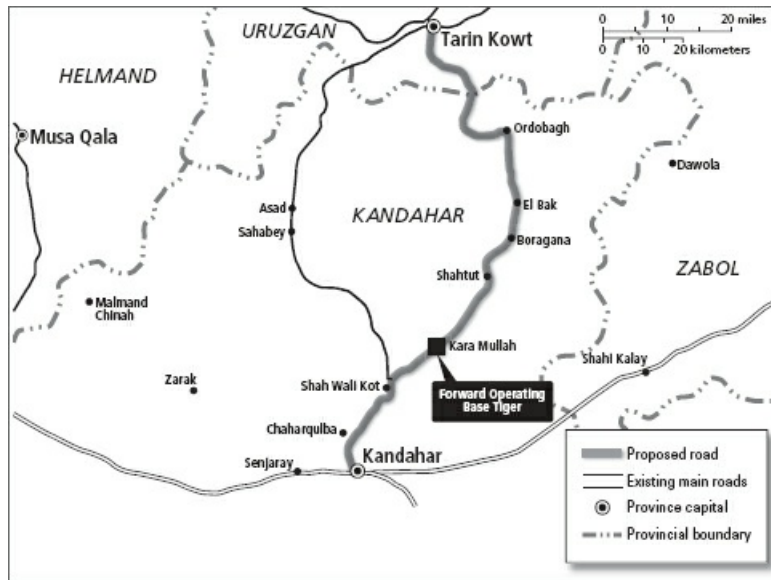
The engineers would have to step up the pace of road building if they were to complete another 70.5 kilometers in only five months. The Army usually builds roads efficiently, but at a pace of a few hundred meters a day. Doing so involves a multistep, mostly sequential process of route planning, surveying, ensuring job site security, sustaining the flow of materiel and water, and maintaining the heavy engineering equipment. To ensure the final integrity of the road, the engineers begin by using dozers to clear grub and remove topsoil, including brush and small hills. Graders level the path to create a suitable foundation. The engineers scout the area to find a source of appropriate sub-base material. Once this is located, they send the candidate material away for content analysis by a contracting company. If the material is suitable, dump trucks and scrapers use this “borrow pit” to harvest material that they use to build up an eight- to twelve-inch sub-base on the leveled foundation. This material is so important that engineers will opt to continue use of a good borrow pit even if it is a long distance from the job site, sometimes up to five kilometers away. Graders subsequently create a crown in the center of the road to aid water

runoff. A finishing crew uses water trucks to douse the road, and rollers compact the soil. Finding sources of water is just as important as finding good sub-base materials, because it is this last step that molds the dust into a road.²⁸

Translating these procedures to the Kandahar–Tarin Kowt corridor on an accelerated schedule would pose particular problems. In addition to issues surrounding survey, materials, maintenance, and water, job site security would be a continual challenge. Regional conditions meant that dust clouds would billow upward as the engineers worked, signaling the engineers’ presence and making them a static and easily visible target. Although the units would have embedded combat engineers, the long, ninety-minute convoys to and from the job site required by an accelerated schedule would run counter to the engineers’ training in operational security, which calls for the use of varied routes and times. During work, the engineers would have to halt and search all traffic along the route, which would take precious time and resources away from the construction effort and would pose cultural challenges if Afghan women had to be searched.²⁹ Moreover, such searches would not address the threat posed by insurgents who dotted the surrounding hills and whom the engineers themselves could not flush out.

Despite these challenges, the US Army was leaning heavily toward adopting the accelerated schedule for Taskforce Pacemaker in April 2005. Construction on the road had proceeded so far without incident amid the difficult conditions and security risks, and the road could provide an important supply link to US and NATO forces in Uruzgan. Ultimately, victory in Afghanistan depended on demonstrating to its people that the US-backed government was improving their lives in tangible ways, and few projects had greater visibility than modern road systems, where “every cut is a blow to the primary weapons of the Taliban—isolation and hardship.”³⁰ The road would bring clear commercial benefits to a region heavily dependent on imported goods, and in turn these benefits could generate more and more support for the Afghan government. Moreover, a rapid success could deal a critical psychological blow to the insurgents, showing the region what the United States could accomplish inside the Taliban’s heartland on the eve of critically important legislative elections. The potential impact of the project was not lost on anyone: it promised to be, as one US Army engineer put it, “not just an engineering feat...[but] a show of political force.”³¹ (See Map 6.2.)

Map 6.2 ▶ Route between Kandahar and Tarin Kowt



RECOMMENDED READING

Dupree, Louis. *Afghanistan*. Princeton, NJ: Princeton University Press, 1980.

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

THE ROAD TO TARIN KOWT

Structured Analytic Techniques in Action

The goal of a Red Team analysis is to minimize surprise by encouraging divergent, open-minded thinking. This approach can be applied to “exercises, experiments, planning, and strategy.”³² A Red Team in its broadest definition challenges conventional wisdom by checking assumptions; encouraging Devil’s Advocacy; and modeling adversaries’ behaviors at the strategic, operational, and tactical levels.³³ The exact techniques used in a successful Red Team analysis can vary based on such factors as the type of decision or issue at hand, the length of time available to conduct the analysis, and the expertise of the analysts. What is most important is choosing techniques that thoroughly challenge a course of action in order to reveal and redress risks and increase the chances of success.

In this case, the 18 September 2005 Afghan National Assembly election is driving a decision about whether to accelerate construction of the road from Kandahar City to Tarin Kowt. The use of a Key Assumptions Check, Devil’s Advocacy, and Strengths-Weaknesses-Opportunities-Threats (SWOT) analysis can help analysts view the elements of the decision through a variety of prisms to troubleshoot the intended course of action and thereby produce more effective policy results.

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.

Table 6.4 ▶ Key Assumptions Check Template				
Key Assumption	Commentary	Supported	With Caveat	Unsupported

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 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”

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

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

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?

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.

Analytic Value Added. Which issues could undermine the goals of the project, and why?

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 by listing the Strengths, Weaknesses, Opportunities, and Threats that are expected to facilitate or hinder achievement of the objective.

Table 6.5 ► SWOT Template			
	US Strengths	US Weaknesses	
	1.	1.	
	2.	2.	
	3.	3.	

Table 6.5 ► SWOT Template (Continued)			
	Opportunities for the United States	Threats to the United States	
	1.	1.	
	2.	2.	
	3.	3.	

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 with your strategies.

Table 6.6 ► SWOT Second-Stage Analysis Template			
	Use Strengths	Improve Weaknesses	
	1.	1.	
	2.	2.	
	3.	3.	
	Exploit Opportunities	Mitigate Threats	
	1.	1.	
	2.	2.	
	3.	3.	

Analytic Value Added. What steps should the US Army take to prepare for road construction?

NOTES

1. Laura M. Walker, "Task Force Pacemaker Constructing a Road to Democracy," *Army Engineer* (September–October 2005): 19.
2. Vincent C. Fusco, "Eikenberry Takes Command of Coalition Forces in Afghanistan," American Forces Press Service, May 4, 2005, http://osd.dtic.mil/news/May2005/20050504_881.html.
3. Louis Dupree, *Afghanistan* (Princeton, NJ: Princeton University Press, 1980), 127.
4. Thomas H. Johnson and M. Chris Mason, "No Sign of Burst until the Fire," *International Security* 32, no. 4 (2008): 62.
5. US Army, "My Cousin's Enemy Is My Friend: A Study of Pashtun 'Tribes' in Afghanistan," Afghanistan Research Reachback Center White Paper, TRADOC G2 Human Terrain System (Fort Leavenworth, KS: US Army, 2009), 14, <http://smallwarsjournal.com/documents/cousinsenemy.pdf>.
6. Ibid.
7. Dupree, *Afghanistan*.
8. Gilles Dorronsoro, "The Taliban's Winning Strategy in Afghanistan" (Washington, DC: Carnegie Endowment for International Peace, 2009), http://www.carnegieendowment.org/files/taliban_winning_strategy.pdf.
9. Dupree, *Afghanistan*, 249.
10. Ibid.
11. Johnson and Mason, "No Sign of Burst until the Fire," 55.
12. Thomas H. Johnson and M. Chris Mason, "Understanding the Taliban and Insurgency in Afghanistan," *Orbis* 51, no. 1 (2007): 88.
13. Dorronsoro, "The Taliban's Winning Strategy."
14. Matthew Nasuti, "The Ring Road: A Gift Afghanistan Cannot Afford," *Kabul Press*, September 29, 2009, <http://kabulpress.org/my/spip.php?article4093>.
15. Johnson and Mason, "Understanding the Taliban," 74.
16. Ibid., 71–89.
17. Dorronsoro, "The Taliban's Winning Strategy"; Greg Mills, "Kandahar through the Taliban's Eyes," *Foreign Policy*, May 27, 2010, http://www.foreignpolicy.com/articles/2010/05/27/kandahar_through_the_talibans_eyes/.
18. Johnson and Mason, "Understanding the Taliban."
19. Dupree, *Afghanistan*.
20. Ibid., 644.
21. 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, <http://www.gao.gov/products/GAO-08-689/>.
22. Ibid.
23. Ibid.
24. Ibid., 4.
25. Dorronsoro, "The Taliban's Winning Strategy."
26. US Government Accountability Office, *Afghanistan Reconstruction Progress*, 11.
27. Walker, "Task Force Pacemaker Constructing a Road to Democracy," 20–24.
28. Ibid.
29. Ibid., 24.
30. Ibid.
31. Ibid., 24.
32. Defense Science Board, *Report of the Defense Science Board 2008 Summer Study on Capability Surprise. Vol. I: Main Report* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2009), <http://www.acq.osd.mil/dsb/reports/ADA506396.pdf>.
33. Defense Science Board, *Defense Science Board Task Force on the Role and Status of DoD Red Teaming Activities* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics), 2003, <http://www.fas.org/irp/agency/dod/dsb/redteam.pdf>.

7 Who Murdered Jonathan Luna?

Key Questions

- ▶ Why would someone target Jonathan Luna for murder?
- ▶ What are the most important controversies surrounding the case?
- ▶ What is the most important evidence in the case?
- ▶ What additional information should law enforcement authorities seek out?

CASE NARRATIVE

Jonathan Luna was an energetic and affable federal prosecutor whose death in December 2003 shocked his friends and colleagues. Luna's story is one of professional and personal success; by the time of his death in 2003, he had risen from his modest roots in New York to become an assistant US attorney in Baltimore, Maryland, near which he lived with his wife and two small children. But in the early hours of 4 December 2003, Luna's body—riddled with thirty-six stab wounds—was found face down in a creek in rural Lancaster County, Pennsylvania, his car still idling nearby. A multiyear, multistate investigation ensued, the public details of which ignited controversy about just how and why Jonathan Luna died.

The Investigation Begins

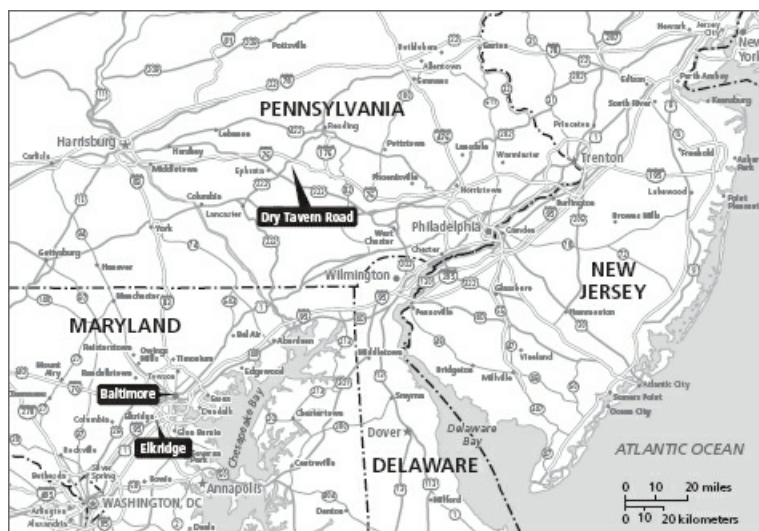
Upon finding Luna's badly beaten and stabbed body, state and federal authorities immediately opened an investigation and fanned out across the region in the hope of tracking down clues that might lead them to the killer.

Investigators combed the area off the two-lane Dry Tavern Road near Denver, Pennsylvania, where a Sensening & Weaver employee had found Luna's car at about 0530 on 4 December 2003.¹ The rural area is about a mile off the Pennsylvania Turnpike and about seventy miles northeast of Baltimore.² Authorities arriving at the scene found Luna's 2003 Honda Accord nose down in a creek and still idling.³ On the exterior of the car, blood was smeared on the driver's side door and left front fender.⁴ Inside the vehicle, money and cell phone equipment were scattered throughout, and a large pool of blood had accumulated on the right rear floor.⁵ Luna's body lay in the creek.⁶ (See Map 7.1.)

Within the first forty-eight hours, more than one hundred police cadets searched the surrounding area for clues, and details began to emerge about the cause of death.⁷ Lancaster County coroner Barry Walp said that Luna was found fully clothed in his suit, shirt and tie,

overcoat, socks, and shoes, along with his wallet, cash, and work identification badge.⁸ A Pennsylvania State Police affidavit quoted in press reports indicated that Luna had suffered a “traumatic wound to the right side of his head,” while other press reports citing a federal law enforcement source said that some of Luna’s thirty-six stab wounds were defensive in nature.⁹ Walp, however, said he did not observe any defensive wounds during the autopsy and that Luna’s wounds were in the neck and upper chest.¹⁰ Although investigators found no weapon at the scene, they said that Luna’s wounds were consistent with a small blade, possibly a penknife.¹¹ There were also signs that he had been restrained and had sustained injuries to his genitals, according to law enforcement sources.¹² Ultimately, Walp assessed that Luna had died from drowning.¹³

Map 7.1 ▶ Jonathan Luna’s Home, Work, and Location of Body



Jonathan Luna’s home in Elkrige was not far from his workplace at the US District Courthouse in Baltimore. His body was found lying with his face in a creek just off of Dry Tavern Road near Denver, Pennsylvania.



FBI photo of Jonathan Luna’s car.

In Baltimore, federal authorities descended upon the US District Courthouse, where building records indicated Luna had been present as late as 2330 the night before.¹⁴ They immediately began to comb through Luna's work files, and they spoke with his colleagues and family members as they tried to piece together his last hours.

The Federal Bureau of Investigation (FBI), along with Luna's boss, US Attorney Thomas M. DiBiagio, held a press conference in which they vowed to find and "bring those responsible for this tragedy to justice."¹⁵ They declined to cite possible motives or suspects, but initial press reports noted the curious timing of his death; Luna was scheduled to be in court as lead prosecutor in the trial of two allegedly violent drug traffickers on the morning his body was found, and he had been working on the plea bargain at the courthouse the night of his death.¹⁶

An Impressive Rise

Jonathan Luna ascended from a less than privileged upbringing in the rough Mott Haven neighborhood in the Bronx, New York, where he lived with his parents, Paul and Rosezella Luna, and his brother David. In a 1991 letter to the *New York Times*, Luna defended his neighborhood and praised his parents' tenacity and hard work, saying, "You and your readers should know that there are decent, hard-working people like my parents who are struggling every day to make a life for themselves and their families in Mott Haven."¹⁷

He went on to beat the odds by attending Fordham University and the University of North Carolina Law School, where he served as class president and graduated in 1992.¹⁸ After law school, he worked as a staff attorney with the Federal Trade Commission in Washington, D.C., and as an assistant district attorney in Brooklyn, New York.¹⁹ In 1999, he landed a job in the US Attorney's Office in Baltimore, Maryland. Then-US Attorney Lynne Battaglia hired him for the job and shortly after his death remembered the "excitement and idealism" he brought to her office.²⁰

At the time of his death, the thirty-eight-year-old prosecutor lived with his wife and two young sons in Elkridge, Maryland, about ten miles from his office at the Federal District Court Building in Baltimore. According to family members, who described the pair as "the perfect couple," they doted on their sons.²¹ Luna's parents remember him as a loving father, husband, and son who helped support them and visited them every week with his children.²² Immediately following his death, the family issued a statement expressing shock, deep grief, and sadness; his parents said that they believed his death was related to his work prosecuting violent criminals.²³

A Likely Victim?

Luna's work for the US Attorney's Office often put him in contact with the region's more unsavory characters. During the twelve months prior to his death, Luna had prosecuted cases involving prostitution, child stalkers, bank robbers, and violent drug offenders. In one high-profile case, he prosecuted a US Navy physicist who allegedly used the Internet to seek out underage girls for sexual encounters. He also won convictions in a case involving a series of violent bank robberies across Baltimore.²⁴

On the morning of 3 December, Luna was in the midst of prosecuting Baltimore-based rap musician Deon Lionnel Smith and his associate, Walter Oriley Poindexter, on conspiracy charges involving the use of their Stash House Records studio to operate a violent drug ring and distribute heroin.²⁵ The day had not started well. Luna was late to court for the third day of the

trial, citing a late-night trip to the hospital with a sick child. Judge William Quarles admonished him and fined him \$25.²⁶ Next, a key witness who was an FBI informant with a criminal past changed his story on the stand.²⁷ In the face of this setback, Luna worked with defense attorneys to reach a deal. Late in the day on 3 December, Poindexter agreed to plead guilty to three counts of the lesser crime of heroin distribution, and Smith agreed to plead guilty to one count each of heroin distribution and possessing a firearm during a drug transaction.²⁸ Luna agreed to drop the conspiracy charges and not to raise evidence at sentencing that linked Poindexter to a fatal shooting.²⁹



FBI photo of Jonathan Luna.

Smith's attorney, Kenneth Ravenell, told reporters that he saw Luna at the courthouse at 1730, shortly after negotiating the plea agreement.³⁰ Ravenell dismissed the possibility of Smith's involvement in Luna's death, pointing out that Smith and Poindexter remained in jail at the time of the murder, and said it would be "just silly of these men to have been involved in this murder because they got what they wanted from their plea."³¹ Poindexter's attorney, Arcangelo Tuminelli, said that he received a call from Luna around 2100; he said Luna told him he was returning to the office to finish paperwork for the plea agreement and would try to fax the agreements to both defendants' lawyers by morning.³² Tuminelli said that it was "implausible" that either defendant would have wanted to harm Luna because they had "every incentive to want to see Jonathan Luna show up [at court] today" to enter the plea agreement.³³ In fact, Luna himself had urged reporters that evening to be on time the next morning.³⁴

Upon hearing of Luna's death, Judge Quarles noted that "prosecutors have two sources of danger in their lives—they are subject to any random act of violence, just like the rest of us, and they are targets to people who have grudges against them. When any prosecutor dies, you can't exclude either possibility."³⁵

Piecing Together Luna's Final Hours

Authorities zeroed in on Luna's work, investigating the possibility that he may have been killed in connection with the case.³⁶ FBI agents were waiting outside the courtroom on 4 December to

question Poindexter's and Smith's family members.³⁷ But law enforcement sources quickly pointed out that they were also examining a range of non-work-related scenarios. A joint task force of state and federal authorities worked during the ensuing weeks and months to compile a clearer picture of Luna's movements during his final hours. Their work revealed the following:

Sometime after 2300 on 3 December Luna received a cell phone call and told his wife he had to return to the office.³⁸ He left home shortly thereafter. Police officers searching his office on the morning of 4 December found his office lights and computer on, with the half-finished plea bargain on the screen. His glasses and cell phone were on his desk.³⁹ Building records indicate that Luna's car left the courthouse parking garage at 2338.⁴⁰

Luna's car, equipped with an electronic toll payment transmitter, E-ZPass, headed northbound on Interstate 95 and passed through the Fort McHenry Tunnel toll gate at 2349.⁴¹ The car, still traveling northbound, passed through the Perryville, Maryland, toll plaza at 0028 and the Delaware Line toll plaza at 0046.⁴²

Luna's debit card was used at the JFK Plaza in Newark, Delaware, at 0057⁴³ to make a \$200 ATM withdrawal, but security cameras did not capture that transaction.⁴⁴ At approximately 0237 the car entered the New Jersey Turnpike at Exit 6A from Route 130.⁴⁵ Tolls on that section of the turnpike are only taken westbound (New Jersey to Pennsylvania), so there is no electronic record of the car crossing from Delaware to New Jersey or from New Jersey to Pennsylvania.

At 0247, Luna's car entered the Pennsylvania Turnpike at Exit 359, the Delaware River Bridge.⁴⁶ It then exited the Pennsylvania Turnpike and reentered, picking up a paper toll ticket rather than passing through the E-ZPass lane.⁴⁷

At 0320, Luna's credit card was used at a Sunoco gas station along the Pennsylvania Turnpike in King of Prussia, Pennsylvania, in the western suburbs of the metropolitan Philadelphia area.⁴⁸ Employees at the Sunoco station said he bought gasoline for two cars, two sodas, and a bottle of water, but authorities found no sign of him on the grainy video surveillance tapes, and investigators said they were "about 99 percent sure" there was not a second car traveling with him, according to a law enforcement source.⁴⁹ Another employee said he had seen Luna at about 0300 when he purchased drinks, saying Luna did not appear to be under any duress and "was just very calm. He must have been with people, but I don't think he knew they were going to kill him."⁵⁰

A Roy Rogers restaurant manager at a rest stop in Elverson, Pennsylvania, thirty miles west, said she saw Luna there before 0330.⁵¹ She said that she remembered that he looked like television host Bryant Gumbel.⁵² She did not recall seeing anyone else with him.⁵³ The FBI would not comment on the report.⁵⁴

Twenty miles and two exits west of Elverson, Luna's vehicle exited the Pennsylvania Turnpike at the Reading-Lancaster interchange, Exit 286, near Ephrata, Pennsylvania, at 0404.⁵⁵ The driver handed over a paper ticket rather than use the E-ZPass lane.⁵⁶

At 0530, Luna's body was discovered off Dry Tavern Road in Lancaster County, Pennsylvania, after a Sensening & Weaver employee reported an unknown car on company property, its engine still idling.⁵⁷

According to Walp, Luna was alive when he arrived at the scene and died of freshwater drowning. Walp classified the death a homicide.⁵⁸

Questions Arise

As authorities combed the scene of the crime, Luna's workplace, and Luna's home; interviewed his friends, family, and coworkers; and tracked down hundreds of possible leads, they began to uncover information that raised important questions about Luna's life and work.

Luna's financial records revealed that he had financial problems, some of which he had kept from his wife. He had run up \$25,000 in credit card debt on as many as sixteen credit cards, which prompted investigators to reopen an investigation into the unsolved disappearance of \$36,000 used as evidence in a bank robbery that Luna had prosecuted in 2002.⁵⁹ An online loan application Luna filled out at about the time of that trial intrigued investigators.⁶⁰ They found that Luna had applied for a loan of about \$30,000 but canceled the application not long after the evidence money went missing.⁶¹

Luna's computer data revealed another set of questions. Although Luna's caseload included the prosecution of online child pornography and child predators, a law enforcement official said federal agents found adult pornographic files on Luna's Justice Department computer that appeared unrelated to his caseload.⁶² They also examined his relationships with two women and, separately, uncovered messages posted by a Jonathan Luna on an online dating website.⁶³ In one post, the individual posting as Jonathan Luna said he was a thirty-one-year-old black male seeking a white, preferably blonde or redheaded, female for sexual encounters.⁶⁴

Authorities also discovered that Luna had made frequent trips to the Philadelphia area, often at odd hours. A gas station employee on the Pennsylvania Turnpike said she saw Luna at the station late at night about once a month over a six-month period.⁶⁵ Luna's father told authorities that Luna had traveled to the Philadelphia area several times in the month preceding his death. Paul Luna said his son even canceled a Thanksgiving weekend trip to New York City in order to travel to Pennsylvania for work.⁶⁶ Luna's colleagues dismissed the possibility that Luna could have been engaged in indiscriminate activities on such trips, pointing out that Luna went to Philadelphia several times to interview the key witness in the case of Smith and Poindexter, who were being detained there.⁶⁷

In addition to investigating possible financial problems and allegedly indiscriminate personal behavior, authorities pursued information that Luna's work situation was apparently suffering as well. Several friends and colleagues said that Luna had told them he felt that his job was in peril and that his relationship with his supervisors in the US Attorney's Office was eroding. He told one friend that he feared he would need to look for a new job.⁶⁸ US Attorney DiBiagio, however, rejected any suggestion that Luna was at risk of being fired, saying "his job was not in jeopardy in any respect."⁶⁹ Instead, DiBiagio lauded Luna's prosecution of a rare pornography production case and noted that Luna had not expressed concerns about his job security at an employee review meeting in June.⁷⁰

New Information Emerges

As the investigation continued, evidence emerged that apparently led investigators to consider a range of alternative motives and suspects. Authorities refused in the initial months of the investigation to comment on possible suspects, but law enforcement sources did state that "since his death, investigators have addressed and covered over 1,000 leads, including neighborhood canvasses, physical searches, review of financial and telephone records, [E-ZPass] travel information, and the analysis of over 10 [gigabytes] of computer data."⁷¹

Although they refused to release the autopsy report, some law enforcement sources said that injuries to Luna's genitals suggested a "highly personal" motive behind the crime.⁷² Also, the fact that he left both his cell phone and his eyeglasses in his office on the night of his murder led investigators to speculate that Luna may have known his attacker.⁷³ However, Walp said Luna had a number of shallow "prick" marks on his chest and neck in addition to several deeper, more serious stab wounds. Press reports suggested that the prick marks are sometimes the result of "hesitation wounds" in suicide cases that involve stab wounds.⁷⁴ Another press report raised the possibility that the prick marks could suggest that Luna was tortured.⁷⁵ According to three law enforcement sources, authorities believed that the motivation behind Luna's wounds was "personal."⁷⁶

In February, during another search of the area where Luna's body was found, investigators found a penknife that they believed was not only the weapon used to make the stab wounds but also the penknife that Luna regularly carried.⁷⁷ They also found blood on the paper toll-booth ticket that was turned in at the exit near Ephrata.⁷⁸ Anonymous law enforcement sources said that authorities found blood from a second person in Luna's car, but investigators never released any information about the alleged evidence of a second person.⁷⁹

Controversy Ensues

The FBI field office in Baltimore pursued the case for more than a year but did not publicly identify any suspects or make any arrests. By December 2004, the case took a strange turn when the FBI released a statement that Luna was alone from the time he left his office on 3 December 2003 until his body was found on 4 December 2003.⁸⁰ The statement implied, without rendering a clear judgment, that the death was a suicide. Lancaster County coroner Gary Kirchner, who took over after Walp retired in January 2004 and whose office conducted Luna's autopsy, rejected the suicide theory and said he was "at least 98 percent" certain that Luna's death was a homicide.⁸¹ Luna's mother also rejected the suicide theory, saying, "He wouldn't do something like that."⁸² Fellow prosecutor Jacabed Rodriguez-Coss said she could "never see Jonathan ever committing suicide."⁸³ Years later, Luna's friend, attorney Richard Reuland, also questioned the defensive wounds explanation, telling reporters, "Some of these wounds, he would have had to have been double- or triple-jointed to inflict on himself. Some of these wounds were in the middle of his back."⁸⁴

The FBI pronouncement served as the capstone on a year of controversy. First, there were reports of the FBI's possible mishandling of a witness in the case while investigating whether the witness, who was also an FBI agent, had engaged in an affair with Luna. Press reports cited rumors that the FBI may have investigated the alleged affair and that the two may have gone to the gym together a few times.⁸⁵ The witness balked at the treatment, and an internal FBI inquiry ensued. The FBI released a statement in February 2004 saying that "any time an FBI employee makes a serious allegation of wrongdoing against a manager or fellow employee, the matter is investigated by independent investigators."⁸⁶

Next, reports surfaced that US Attorney DiBiagio admitted to staff members in a meeting in August 2004 that he had lied to the news media about whether Luna's job was in jeopardy to protect Luna's family, according to employees in the US Attorney's Office.⁸⁷ Finally, in 2005, a source close to the investigation revealed that Luna was scheduled for a polygraph examination concerning the missing \$36,000 from the bank robbery case.⁸⁸ The source said that investigators

found that more than \$10,000 mysteriously came into Luna's possession just after the money went missing.⁸⁹ The FBI declined to comment on the reports, but the revelations prompted speculation that Luna may have accidentally killed himself when staging his own abduction to generate sympathy and stall the polygraph examination.⁹⁰

William Keisling fueled the controversy and provided fodder for conspiracy theorists in a 2005 book, *The Midnight Ride of Jonathan Luna*. In it, Keisling argued that Luna's death was most likely associated with his profession, claiming Luna had frustrations surrounding the FBI's alleged mishandling of its informant in the Smith and Poindexter case.⁹¹ Likewise, the Luna family's private investigator believes that Luna's professional life—including his dealings with the FBI informant—should again be the focus of the case.⁹² The FBI case is still open, but authorities have not issued any public statements since 2004, the same year it offered a \$100,000 reward for information leading to the “resolution of the investigation” into Luna's death.⁹³

An Unsolved Mystery

Jonathan Luna's mysterious death in December 2003 has been widely reported, but attempts to reignite the investigation have stalled. It has been the subject of national attention and two nonfiction books. And yet the mystery has never been solved. Vigils in his honor have become increasingly rare. His family has fallen silent after unsuccessfully attempting in 2007 to persuade the state of Pennsylvania to open an inquiry into his death. The US Attorney's Office for the Eastern District of Pennsylvania in 2008 was unsure if it was still overseeing the case.⁹⁴ The question remains: How did Jonathan Luna die?

RECOMMENDED READINGS

Brown, Ethan. *Snitch: Informants, Cooperators, and the Corruption of Justice*. New York: PublicAffairs, 2007. See chapter 7.

Keisling, William. *The Midnight Ride of Jonathan Luna*. Harrisburg, PA: Yardbird, 2006.

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

WHO MURDERED JONATHAN LUNA?

Structured Analytic Techniques in Action

When confronting a case in which so much significant information is unknown, Timelines, Chronologies, Hypothesis Generation, and Analysis of Competing Hypotheses can be used to devise and execute a solid analytic process that frames the problem and brings order to the jumble of data points, assumptions, and gaps that form the case. The following exercises use these techniques to sort, array, and analyze the data set in a way that can bring this complex set of events into better focus.

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?

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

- Are there any missing pieces of data?
- 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?
- Could any events outside the Timeline have influenced the activities?
- Are there any underlying assumptions about the evidence that should be taken into consideration?

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.

Analytic Value Added. What does the sequence of events tell you? Are there any gaps in the information that should be addressed? What additional information should you seek? How confident are you in the sources of information?

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 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.
- STEP 3:** Aggregate the hypotheses into affinity groups and label each group.
- STEP 4:** Use problem restatement and consideration of the opposite to develop new ideas.
- STEP 5:** Update the list of alternative hypotheses.
- STEP 6:** Clarify each hypothesis by asking, Who? What? How? When? Where? and Why?
- STEP 7:** Select the most promising hypotheses for further exploration.

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.

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?
- STEPS 2 AND 3:** Identify plausible alternatives for each key component and strive to keep them mutually exclusive. Discard any “given” factors.
- STEPS 4, 5, AND 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.
- STEP 7:** Re-sort the remaining hypotheses, listing them from most to least credible.
- STEP 8:** Restate the permutations 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.

Analytic Value Added. Which hypotheses should be explored further? What motives should be considered, and why? Which hypotheses from the original list were set aside, and why?

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 Pherson Associates 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.

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.

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?

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.

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.

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

STEP 9: Identify indicators or milestones for future observation.

Analytic Value Added. As a result of your analysis, what are the most and least likely hypotheses? What are the most diagnostic pieces 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? Why do you think that the case remains unsolved?

NOTES

1. Gail Gibson, “Prosecutor of Drug Case Found Killed,” *Baltimore Sun*, December 5, 2003, <http://www.baltimoresun.com/news/maryland/crime/bal-luna1205,0,2335211.story>; “Jonathan Luna’s Last Hours,” *Washington Post*, March 14, 2004, <http://www.washingtonpost.com/>.

2. Gibson, “Prosecutor of Drug Case Found Killed.”

3. Gail Gibson, “Personal Motive Suspected in Killing of US Prosecutor,” *Baltimore Sun*, December 6, 2003, <http://www.baltimoresun.com/news/maryland/crime/bal-luna1206,0,2400748.story>.

4. Ibid.

5. Ibid.

6. Gibson, "Prosecutor of Drug Case Found Killed."
7. Ibid.
8. Gibson, "Personal Motive Suspected in Killing of US Prosecutor"; Lauren Johnston, "Prosecutor May Have Been Tortured," *CBS News*, December 6, 2003, <http://www.cbsnews.com/stories/2003/12/08/national/main587250.shtml>.
9. Gibson, "Personal Motive Suspected in Killing of US Prosecutor."
10. Lauren Johnston, "New Puzzle in Prosecutor's Death," *CBS News*, December 12, 2003, <http://www.cbsnews.com/stories/2003/12/04/national/main586958.shtml>.
11. Gail Gibson, "Blood of Second Person in Car," *Baltimore Sun*, December 12, 2003, <http://www.baltimoresun.com/news/maryland/bal-md.luna12dec12,0,1042873.story>.
12. Gail Gibson and Lynn Anderson, "Missing Money Noted in Probe," *Baltimore Sun*, December 10, 2003, <http://www.baltimoresun.com/news/maryland/bal-md.luna10dec10,0,125365.story>.
13. Gibson, "Personal Motive Suspected in Killing of US Prosecutor."
14. Gibson, "Prosecutor of Drug Case Found Killed."
15. Ibid.
16. Ibid.
17. Ibid.
18. Ibid.
19. Ibid.
20. Ibid.
21. Gail Gibson and Gus G. Sentementes, "Decision in Slaying Probe Set for Today," *Baltimore Sun*, December 8, 2003, http://articles.baltimoresun.com/2003-12-08/news/0312080348_1_luna-body-law-enforcement/.
22. Gus G. Sentementes, "Luna Parents Wait, Hope for Word on Son's Killer," *Baltimore Sun*, December 11, 2003, <http://www.baltimoresun.com/>.
23. Gibson, "Blood of Second Person in Car"; Gail Gibson, "Slain Prosecutor's Relationships with Women Examined," *Baltimore Sun*, December 9, 2003, http://articles.baltimoresun.com/2003-12-09/news/0312090426_1_luna-law-enforcement-lancaster-county/.
24. Ibid.
25. Faye Fiore, "Missing Federal Attorney Found Slain," *Los Angeles Times*, December 5, 2003, <http://articles.latimes.com/2003/dec/05/nation/na-luna5/>.
26. Gibson, "Personal Motive Suspected in Killing of US Prosecutor."
27. Tricia Bishop, "Five Years Later, Prosecutor's Death Still a Mystery," *Baltimore Sun*, November 30, 2008, <http://www.baltimoresun.com/news/maryland/bal-md.luna30nov30,0,2938855.story>.
28. Gibson, "Prosecutor of Drug Case Found Killed."
29. Ibid.
30. Kenneth Ravenell, interviewed by Wolf Blitzer, *PM Edition*, CNN, December 5, 2003, <http://edition.cnn.com/TRANSCRIPTS/0312/05/wbr.00.xlink.html>.
31. Ibid.; Eric Lichtblau, "Federal Prosecutor Found Dead with Stab Wounds," *New York Times*, December 5, 2003, <http://www.nytimes.com/2003/12/05/national/05PROS.html>.
32. Gibson, "Prosecutor of Drug Case Found Killed."
33. Ibid.
34. Gibson, "Personal Motive Suspected in Killing of US Prosecutor."
35. Gibson, "Prosecutor of Drug Case Found Killed."
36. Eric Rich and Allan Lengel, "FBI Finds No Culprit in Death of Prosecutor; Probe Suggests Luna Was Alone," *Washington Post*, December 3, 2004, <http://www.washingtonpost.com/>; Gibson, "Prosecutor of Drug Case Found Killed."
37. Ibid.
38. Gibson, "Personal Motive Suspected in Killing of US Prosecutor."
39. *Brooklyn Eagle*, April 25, 2011.
40. "Jonathan Luna's Last Hours," *Washington Post*, March 14, 2004, <http://www.washingtonpost.com/>.
41. Ibid.
42. Ibid.
43. Ibid.
44. Gail Gibson, "Blood Found on Slain Prosecutor's PA Toll Ticket," *Baltimore Sun*, December 17, 2003, <http://www.baltimoresun.com/news/maryland/bal-md.luna17dec17,0,3336643.story>; Gail Gibson and Lynn Anderson, "Probe in Killing of Prosecutor Luna Stalls," *Baltimore Sun*, January 9, 2004, <http://www.baltimoresun.com/news/maryland/crime/bal-probe0109,0,5329212.story>.
45. "Jonathan Luna's Last Hours."

46. Ibid.
47. Gibson, "Blood of Second Person in Car."
48. "Jonathan Luna's Last Hours"; Gibson, "Blood Found on Slain Prosecutor's PA Toll Ticket."
49. Gibson, "Blood of Second Person in Car"; Gibson, "Blood Found on Slain Prosecutor's PA Toll Ticket"; Matt Apuzzo, "Slain Prosecutor's Route Home Adds to Mystery," *Red Orbit*, December 14, 2003, http://www.redorbit.com/news/oddities/35770/slain_prosecutors_route_home_adds_to_mystery/index.html.
50. Gibson, "Blood of Second Person in Car."
51. Apuzzo, "Slain Prosecutor's Route Home Adds to Mystery."
52. Ibid.
53. Ibid.
54. Ibid.
55. "Jonathan Luna's Last Hours."
56. Gibson, "Blood Found on Slain Prosecutor's PA Toll Ticket."
57. "Jonathan Luna's Last Hours."
58. Bishop, "Five Years Later."
59. Rich and Lengel, "FBI Finds No Culprit in Death of Prosecutor"; Eric Rich and Allan Lengel, "Polygraph Loomed for MD Lawyer," *Washington Post*, December 20, 2005, <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121901827.xlink.html>; Stephanie Hanes, "Luna Reportedly Feared Losing Job, Hired Lawyer," *Baltimore Sun*, August 18, 2004, <http://www.baltimoresun.com/news/maryland/bal-md.luna18aug18,0,7793110.story>.
60. Rich and Lengel, "Polygraph Loomed for MD Lawyer."
61. Ibid.
62. Gibson, "Slain Prosecutor's Relationships with Women Examined."
63. Ibid.
64. Ibid.
65. Rich and Lengel, "FBI Finds No Culprit in Death of Prosecutor."
66. Gibson and Sentementes, "Decision in Slaying Probe Set for Today."
67. Gibson, "Blood of Second Person in Car."
68. Gibson, "Slain Prosecutor's Relationships with Women Examined."
69. Rich and Allan, "FBI Finds No Culprit in Death of Prosecutor."
70. Gibson, "Slain Prosecutor's Relationships with Women Examined."
71. Rich and Lengel, "FBI Finds No Culprit in Death of Prosecutor."
72. Gibson and Sentementes, "Decision in Slaying Probe Set for Today."
73. Gibson, "Personal Motive Suspected in Killing of US Prosecutor."
74. Gail Gibson, "Search Uncovers Luna's Penknife," *Baltimore Sun*, February 13, 2003, <http://www.baltimoresun.com/news/maryland/bal-md.luna13feb13,0,1960380.story>.
75. Johnston, "Prosecutor May Have Been Tortured."
76. Gibson, "Personal Motive Suspected in Killing of US Prosecutor."
77. Gibson, "Search Uncovers Luna's Penknife."
78. Gibson, "Blood Found on Slain Prosecutor's PA Toll Ticket."
79. Gibson, "Blood of Second Person in Car."
80. Rich and Lengel, "FBI Finds No Culprit in Death of Prosecutor."
81. Ibid.
82. Ibid.
83. Rich and Lengel, "Polygraph Loomed for MD Lawyer."
84. Samuel Newhouse, "Luna's Last Ride after Leaving Brooklyn D.A.'s Office, Federal Prosecutor's Life Takes Unexpected and Deadly U-Turn," *Brooklyn Daily Eagle*, April 25, 2011, http://50.56.218.160/archive/category.php?category_id=4&id=42954.
85. Ibid.
86. "Statement of FBI Assistant Director Cassandra M. Chandler," February 12, 2004, <http://www.fbi.gov/news/pressrel/press-releases/statement-of-fbi-assistant-director-cassandra-m.-chandler/>.
87. Hanes, "Luna Reportedly Feared Losing Job, Hired Lawyer."
88. Rich and Lengel, "Polygraph Loomed for MD Lawyer."
89. Ibid.
90. Ibid.
91. William Kiesling, *The Midnight Ride of Jonathan Luna* (Harrisburg, PA: Yardbird Press, 2005).

92. Bishop, "Five Years Later."
93. Ibid.
94. Ibid.

8 The Assassination of Benazir Bhutto

Key Questions

- Who would want to kill presidential candidate Benazir Bhutto, and why?
- In what ways would the perpetrator benefit from her death?
- Who would want to see her die, and why?
- How difficult would it be to assassinate her?
- How long would it take to mount such an operation?
- What are the most likely political consequences of her death?

CASE NARRATIVE

Only two months after Benazir Bhutto returned from exile to Pakistan to take up the family's political banner, she was assassinated on 27 December 2007 as her caravan departed a political rally in Rawalpindi, just south of Islamabad. Bhutto had been warned not to return to Pakistan to run for the presidency and, after she returned, had earlier been denied permission to hold a rally in Rawalpindi because of the tenuous security situation. Bhutto, however, refused to be intimidated by the numerous threats on her life and saw such political rallies as key to demonstrating popular support for her candidacy in upcoming presidential elections. The suicide-bomber assassin was later identified as a fifteen-and-a-half-year-old teenager, but questions remained about who had ordered the killing. The list of potential masterminds was not short. It included Islamic militant extremists, political rivals, senior officials in the Pakistani government, and even family members. The event and subsequent investigations captured the attention of the world, while both experts and amateurs sought to determine who ultimately was responsible for her death.

Intertwining Politics and Family

Pakistan has suffered a history of political turbulence since its genesis in 1947. No elected government has survived until the end of its term since the nation was created as a homeland for Muslims during the British partition of South Asia. The main fault lines, then and now, run between secular and fundamentalist Muslims and between civilian leaders and the military.¹

Benazir Bhutto personified this political turmoil. The military ousted her father as prime minister in 1979, convicted him of complicity in the death of a political opponent, and hanged him.² The family was forced into exile. In 1986, Bhutto returned from exile in England to head

the secular Pakistan People's Party (PPP), founded by her father. She led the party to victory in 1988, becoming the first female prime minister of a Muslim country. The Pakistani president dismissed her in 1990 for alleged corruption and her failure to curb ethnic violence. She regained office in 1993.

Violence continued to plague members of the Bhutto family even during Bhutto's years in office. Her brother, Murtaza, who challenged her for control of the PPP, was gunned down near his home by police in 1996.³ His daughter, Fatima, has since called the attack a carefully planned assassination in which Murtaza was allowed to bleed to death after being shot at close range. Fatima, now a newspaper columnist and pro-democracy activist in Karachi, holds Benazir morally responsible for Murtaza's death. In 1996, Bhutto was once again dismissed from office for alleged corruption.⁴ She was later convicted in 1999 for failing to appear in court, but that judgment was subsequently overturned. Facing corruption charges in five separate cases, she fled the country that same year.

Violent Homecoming

Bhutto returned from exile once again on 18 October 2007 after President and Army Chief of Staff Pervez Musharraf signed a "corruption amnesty."⁵ The declaration, drafted under pressure from the White House and the US Congress, not only paved the way for Bhutto's homecoming but also held out at least a vague promise of power sharing.⁶ Another prominent regime opponent, twice-deposed Prime Minister Nawaz Sharif, returned to Pakistan in the fall of 2007; he and Bhutto were longtime political rivals and had no plans to make common cause.⁷

The country was tense after months of protests against the Musharraf government.⁸ Much of the tumult was driven by political bickering surrounding the upcoming presidential elections and a possible return to democracy after more than eight years of military rule. While individual politicians, political parties, and the military all jockeyed with one another for power in advance of the upcoming vote, Islamic militants increased their attacks, seeking to stall the country's sudden move toward democracy. At the same time, the United States and the international community increased pressure on Pakistan to take a more active role in suppressing the Taliban and al-Qaeda. Some observers claimed that the turmoil was driving Pakistan to "the brink" and left it "the main contender for the title of most dangerous country on earth."⁹ (See Map 8.1.)

About two hundred thousand supporters greeted Bhutto at the Karachi airport.¹⁰ The government deployed more than twenty thousand security personnel to maintain order. Despite her personal security worries, Bhutto refused a request by Pakistani authorities to use a helicopter.¹¹ When leaving the airport en route to the tomb of Muhammad Ali Jinnah, the founder of Pakistan, she also decided not to use the bulletproof glass cubicle mounted on her open-air truck. She stood at the front railing surrounded by other party officials.

Map 8.1 ► Pakistan



Benazir Bhutto returns to Pakistan on 18 October 2007 atop an open-air truck. (Bhutto pictured center, with scarf.)

The procession crept forward, with supporters dancing in the streets. Suddenly, there was a small explosion ahead of the truck. It was followed by a large blast near the truck itself, which set an escorting police van on fire and broke windows in Bhutto's vehicle.¹² Bhutto was shaken but not injured in the attack. In all, 179 people were left dead, including several police officers, and more than 600 were injured.¹³ Police officer Raja Khitab later said evidence at the scene pointed to a suicide bombing.¹⁴

Bhutto was well aware of the dangers. Two days before her return to Pakistan, she wrote a letter to Musharraf in which she named four people she believed were plotting to kill her: Ijaz

Shah, current chief of the Intelligence Bureau, which answers to the Interior Ministry; Chaudhry Pervaiz Elahi, former chief minister of the Punjab region; Arbab Ghulam, former chief minister of Sindh; and Hamid Gul, former chief of the Pakistani intelligence service, ISID.¹⁵

After the bombing, Bhutto rephrased her warning and made it public:

On Oct 16, before returning home, I wrote a letter to Gen Musharraf in which I informed him that if anything happens to me as a result of these attacks, then I will neither nominate the Afghan Taliban, nor Al Qaeda, not even Pakistani Taliban or the fourth group. I will nominate those people who, I believe, mislead the people. I have spelt out names of such people in the letter....I have named three people, and more, in that letter to Gen Musharraf. I have named certain people with a view to the attack that took place yesterday so that if I was assassinated, who should be investigated.¹⁶



Probable suicide bombing near Bhutto's bus on 18 October 2007.

According to Mark Siegel, her US representative, Bhutto tried to obtain security personnel from the US firm Blackwater and the UK-based ArmorGroup, but the Pakistani government refused to grant visas.¹⁷

Strident Messages Inflame Opponents

Upon her return to Pakistan, Bhutto used the media to crusade against Islamic militants.¹⁸ She denounced jihadi terrorists with statements that few local politicians had dared to utter. During campaign appearances, she argued that suicide bombing was against the teachings of Islam.¹⁹

Bhutto attacked conservatives in the government, including officials close to Musharraf.²⁰ She accused them of aiding extremists and supporting the bombers who attacked her. Specifically, she warned against ISID and the residual power of those who had been responsible for her father's death. She assailed the military dictatorship in general but stopped short of attacking Musharraf directly, leaving the door open to the proposed power-sharing deal.²¹

Her opponents matched her rhetoric with countercharges. The chief minister of Sindh,

Bhutto's home province, called the rule of a woman a curse for Pakistan. The leader of the Pakistani Muslim League, Chaudhry Hussein—a Musharraf supporter who strongly disapproved of compromise with Bhutto—suggested that the new arrival had arranged the blasts herself as a ploy for sympathy. Ejaj ul-Haq, the minister of religious affairs, blamed Bhutto for playing with people's lives by returning when she was aware of threats against her.²²

Musharraf grudgingly approved her return under US pressure to restore civilian rule, but many Pakistani democrats were skeptical of the image in the Western press of Bhutto as a savior who would rescue the country from autocratic rule and terrorism. Critics on TV talk shows and in newspapers complained that Musharraf had offered amnesty in return for Bhutto's support for an extension of his term in office. Many portrayed the amnesty offer as implicit approval of political corruption. A popular cricketer turned politician, Imran Khan, and his ex-wife, the wealthy British socialite Jemima Khan, lambasted Bhutto in the British press, calling her "a kleptocrat in an Hermès scarf." In a London editorial, Khan highlighted Bhutto's husband's moniker, "Mr. 10 Percent," and accused the two of having stolen more than \$1 billion from the Pakistani treasury during Benazir's second time as prime minister.²³ Opponents also pointed out that she was appealing a money-laundering conviction in the Swiss courts and that corruption investigations were ongoing in Britain and Spain.²⁴

Bhutto's estranged niece Fatima said in an interview after Bhutto's return, "I do believe Benazir is the most dangerous thing to happen to this country."²⁵ She argued that Bhutto's pro-American agenda was giving democracy a bad name and was jeopardizing hard-won progress in grassroots political development. "She has put us all in danger of an Islamic backlash," Fatima declared in the interview. Fatima threatened to ally with other opposition leaders.²⁶

Musharraf, meanwhile, continued his efforts to curtail Bhutto's political campaigning. On 9 November, police erected barbed wire around the Bhutto compound to prevent her from speaking at a rally protesting Musharraf's emergency rule.²⁷ They also rounded up thousands of her supporters. On 13 November, authorities put Bhutto under house arrest, citing concerns for her safety. She responded by calling for Musharraf's resignation and threatening to have her party boycott the elections scheduled for January 2008.

Bhutto's niece considered the complaints about a house arrest to be hollow. She pointed out that Bhutto's political planning was not stifled, and, indeed, more than fifty members of her party were allowed to meet with her during the purported detention.²⁸ Moreover, Bhutto addressed the media twice from her garden, protected by the police, and was not reprimanded for holding a news conference. Bhutto's niece contended that other activists who even mentioned the idea of holding a press conference were jailed.

Bhutto's opponents matched her strident tone. In mid-November 2007, a leaked letter suggested that in 1990 Bhutto had sought to conspire with Pakistan's enemy, India, for political gain. It was common knowledge that Bhutto and then-US ambassador to Croatia Peter Galbraith had been close friends since college days. In the purported letter, Bhutto was alleged to have asked Galbraith to convince the Indian prime minister to create a military incident on the border to put pressure on the Pakistani government and keep it from disqualifying her in upcoming elections. Officials in Bhutto's party denounced the letter as a forgery, citing gross grammatical errors as proof.²⁹

The Final Days

By late December, nerves on all sides were frayed. Bhutto's detention had been lifted, and she had resumed her political campaign.³⁰ After the bombings on the day of her return to Pakistan, she had briefly considered abandoning public rallies and delivering taped messages by TV or radio instead, but she had concluded that mass rallies were crucial to her chances of electoral success. On 26 December, authorities detained a man carrying explosives near one of her rallies in Peshawar, close to the Afghan border.³¹ The man claimed it was celebratory dynamite from a wedding he had attended. Bhutto's husband phoned from Dubai to say he was nervous and wanted to attend the rally planned for the next day in Rawalpindi in her place, but she dissuaded him.³²

The controversial candidate planned to use her 27 December speech to charge that Musharraf intended to rig the elections set for 8 January.³³ She was scheduled to meet during the day with election observers from the European Union, US Senator Arlen Specter, and US Representative Patrick Kennedy. Her plan was to give them evidence that the elections would be fixed through fake polling stations and voter intimidation. Despite her busy day, she met early that morning with Afghan President Hamid Karzai to confer on the growing dangers of extremism.³⁴

Bhutto was apprehensive about her trip to Rawalpindi, just south of the capital. Considered the home of the military, it was where her father had been hanged in 1979 and where Pakistan's first prime minister had been assassinated in 1951.³⁵ Things were already going badly in Rawalpindi. In the early afternoon, a sniper on a rooftop killed four Sharif supporters and injured five others.³⁶ Sharif's party blamed Musharraf's group, claiming the attack was an attempt to intimidate potential voters. Despite the danger, at 1545, Bhutto and her top party officials drove the ten miles from Islamabad to Rawalpindi.

Bhutto held the rally as planned. Near dusk, as she drove away from the site in her bulletproof SUV, she raised her head through the sun roof to acknowledge the frenzied crowds chanting "Long Live Bhutto!"³⁷ Police constable Mohammed Qayyam, who was trying to clear a path for the vehicle, failed to see the man in sunglasses standing just behind Bhutto. Eyewitnesses later reported he raised a gun and fired three shots at close range. Nor did the constable notice the man a few paces back whose head was covered in a white scarf. Witnesses said he blew himself up moments later, killing himself, the likely gunman, and others all around. Bhutto was among those who died.

Bhutto was rushed to Rawalpindi General Hospital, where she was pronounced dead just after 1800.³⁸ The next day her remains were transferred to her husband and flown to Larkana. She was buried in the family's mausoleum that afternoon.

Multiple Accounts in the Aftermath

Controversy immediately swirled, beginning with disagreements over the cause of death.³⁹ Initial reports were that Bhutto had been shot in the head or neck before the bomb went off and had died from the gunshot wounds. The next day, Ministry of Interior officials said she had been killed by shrapnel from the bomb. Two days after the attack, the Interior Ministry issued a more definitive statement, claiming that the shooter had missed but the bomb had caused her to fall; her head had struck a protruding lever on the sun roof, and she died from a skull fracture.⁴⁰ The Interior Ministry official showed X-rays to support this claim. Witnesses and close friends who rushed her to the hospital, however, said she clearly had been shot.⁴¹

Doctors who had attended Bhutto initially reported that she had died of gunshot wounds.

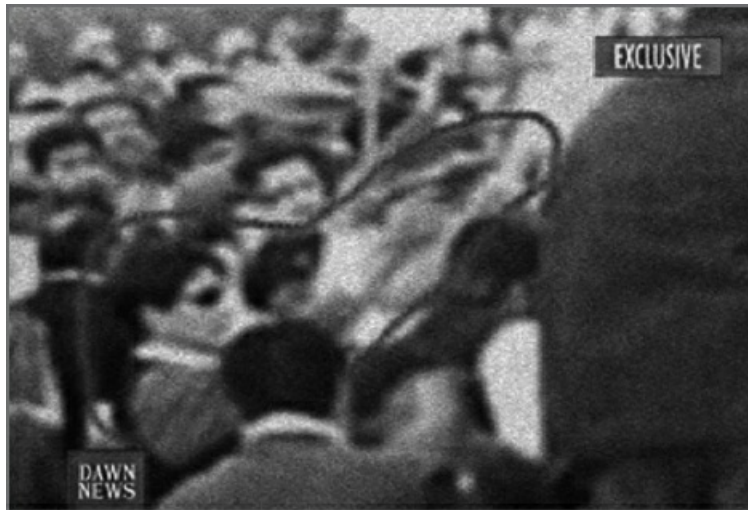
They later released findings consistent with the Interior Ministry's position. One Pakistani doctor said the government had seized Bhutto's medical records and ordered the doctors to stop talking.⁴² A subsequent report issued by a UN team investigating the assassination noted that this doctor was not an attending physician, which caused some to question his credibility.⁴³

There was no autopsy, despite a legal requirement for one in such cases. The government claimed this was in deference to Islamic traditions and Bhutto's husband's wishes.⁴⁴ In response to a government offer to disinter her if her husband so requested, Bhutto's husband declined, saying an autopsy would be useless because the results would be rigged.⁴⁵

An hour and a half after the attack, the senior police officer on the scene ordered police officers to wash down the street with fire hoses. Pools of blood, bullet casings, and DNA samples were all washed away.⁴⁶ Even Hamid Gul, a detractor of Bhutto with connections to both the Afghan and Pakistani Taliban, publicly questioned why the government had washed away evidence at the scene of the crime.⁴⁷ All that remained was amateur footage showing a man in a black vest brandishing what appeared to be a gun and, behind him, a man in a white head scarf believed by some to be the suicide bomber. The government established a joint investigation team headed by local Singh authorities, which later examined the vehicle and reported that it could find no blood or tissue on the hatch where Bhutto was alleged to have struck her head.⁴⁸

Musharraf immediately took steps to distance the government from the assassination. He later acknowledged that Bhutto might have been shot, but he blamed her for poor judgment in ignoring her advisors by standing up in the vehicle, noting that no one else in the car was hurt.⁴⁹ He pointed out that most of the nineteen suicide bombings that had occurred in Pakistan in recent months were directed against the military and the intelligence service.⁵⁰ Discounting stories blaming ISID for the assassination, he stated, "No intelligence organization in Pakistan, I think, is capable of indoctrinating a man to blow himself up."⁵¹ The government had warned Bhutto of the danger of staging a rally in Rawalpindi, he said, and, in fact, had stopped an earlier rally planned for that location by putting her briefly under house arrest. Musharraf claimed security had been as tight as possible on the day of the assassination, with one thousand police officers on duty, including snipers on roofs and mobile squads around Bhutto's vehicle.⁵²

Soon after the attack, the Interior Ministry claimed it had a communications intercept that proved that Baitullah Mehsud, a leader of the Pakistani Taliban thought to be an al-Qaeda affiliate, had instigated the attack (see Figure 8.1).⁵³ Mehsud's forces had been attacking Pakistani military units that were trying, at Washington's behest, to assert control over quasi-autonomous tribal areas where diverse anti-US militants had found sanctuary. The alleged intercept purports to record Mehsud congratulating a follower on a job well done. The US Central Intelligence Agency director, General Michael Hayden, said in late January 2008 that he believed Mehsud was behind Bhutto's assassination. Hayden did not lay out his evidence and made no comment on whether the alleged intercept figured in his calculation. Some wondered whether Hayden's public statement was intended to exonerate Musharraf, a counterterrorism ally.⁵⁴



The top video image shows a man (wearing sunglasses) pointing a gun at Benazir Bhutto on 29 December 2007. The bottom image shows this suspected gunman and the suspected suicide bomber (wearing white scarf).

Figure 8.1 ▶ Communications Intercept Released by the Pakistani Government

Mallah: Peace be with you.

Baitullah Mehsud: And also with you.

Mallah: Chief, how are you?

Baitullah Mehsud: I am fine.

Mallah: Congratulations, I just got back during the night.

Baitullah Mehsud: Congratulations to you, were they our men?

Mallah: Yes, they were ours.

Baitullah Mehsud: Who were they?

Mallah: There was Saeed, there was Bilal from Badar and Ikramullah.

Baitullah Mehsud: The three of them did it?

Mallah: Ikramullah and Bilal did it.

Baitullah Mehsud: Then congratulations.

Mallah: Where are you? I want to meet you.

Baitullah Mehsud: I am at Makeen [town in South Warzistan], come over, I am at Anwar Shah's house.

Mallah: OK I'll come.

Baitullah Mehsud: Don't inform their house for the time being.

Mallah: OK.

Baitullah Mehsud: It was a tremendous effort. They were really brave boys who killed her.

Mallah: Mashallah. When I come I will give you all the details.

Baitullah Mehsud: I will wait for you. Congratulations, once again congratulations.

Mallah: Congratulations to you.

Baitullah Mehsud: Anything I can do for you?

Mallah: Thank you very much.

Baitullah Mehsud: Asalaam Aleikum.

Mallah: Waaleikum Asalaam.

Source: "Pakistan in Crisis: 'Intercept' of al-Qaida Points to Bhutto Plot," World Net Daily, December 28, 2007, <http://www.worldnetdaily.com/index.php?pageId=45282>.

Other US officials agreed that Mehsud was a likely candidate.⁵⁵ The Taliban leader had been critical of both Afghan president Karzai and Pakistani president Musharraf for their close alliance with the United States. He was Pashtun and, like many in the remote tribal area straddling Afghanistan and Pakistan, wanted to see his kinsmen rule a country of their own that followed strict Islamic law and tribal traditions. In 2005, Musharraf had struck a deal with Mehsud, suggesting the two could coexist. Mehsud agreed to halt cross-border attacks into Afghanistan and stop sheltering al-Qaeda and other foreign fighters in return for the withdrawal of Pakistani military forces from Waziristan, his tribal area. He denied that he had been given large bags of cash as a sweetener. Mehsud eventually broke the agreement, allowed foreign fighters back into the safe haven, and resumed operations against the Pakistan Army.⁵⁶

Some observers questioned the intercept's authenticity as too convenient and termed the government's accusation of Mehsud just another case of Pakistan rounding up the "usual suspects" when the police are stumped—the government had named him in previous investigations when it had no leads.⁵⁷ Mehsud quickly and publicly denied any involvement in Bhutto's assassination, just as he had rejected any role in the October bombing when Bhutto first

returned. His spokesperson emphasized that striking a woman violated tribal customs and asserted that the crime was a plot by the government and the intelligence services.

Pakistani security officials arrested a fifteen-year-old, Aitezaz Shah, in the northwest tribal region on the suspicion he was involved in the assassination.⁵⁸ The Al Jazeera news network quoted security sources as saying the teenager had confessed that he was one of five suicide bombers sent to kill Bhutto.⁵⁹ During interrogation, Shah said that two of the attackers, Akram and Bilal, were to target Bhutto first. If they failed, the other three were charged with completing the operation. Bilal killed Bhutto by shooting her and detonating an explosive vest, Shah told officials. He was unable to provide details about the locations of other members of the assassination team.⁶⁰ Members of Bhutto's political party dismissed Shah's arrest, stating it was not the breakthrough the Pakistani government claimed. "Frankly, the arrest of a 15-year-old and his handler is neither here nor there," said Abida Hussain, a senior politician in the party.⁶¹

In her posthumously published book, Bhutto mentioned another possible assassin: Islamic radical Qari Saifullah Akhtar.⁶² Bhutto claimed he had helped procure the bombs that went off in Karachi on 18 October 2007. Akhtar had been arrested previously for participating in an attempted "Islamic coup" against Bhutto's second government and had subsequently forged a relationship with the Taliban and Mullah Omar. Akhtar heads the Harkat-ul-Jihad-al-Islami (HUJI), a group with ties to terrorists in Tajikistan, Chechnya, Burma, Uzbekistan, and Bangladesh.

Scotland Yard Weighs In

As the initial international outcry over the assassination and bungled investigation quieted down, Musharraf asked Scotland Yard on 2 January to send a small team to investigate Bhutto's death.⁶³ The team visited the scene of the crime on 8 January. Musharraf established strict parameters for the Yard's involvement. Investigators were limited to looking into the cause of death, with Pakistani authorities retaining responsibility for identifying the culprit(s). Scotland Yard was denied permission to question some of the people Bhutto's husband accused of plotting to kill her, including several politicians and the intelligence chief.⁶⁴ Scotland Yard examined the gun purportedly used in the attack for fingerprints and linked the prints to the identity card of a man living in Swat, a town in the area controlled by Mehsud. It is unclear whether the Yard was able to match the prints to any of the victims at the scene.

Based on X-rays that were independently verified as Bhutto's (by comparison with dental records) and on reports from the doctors and family members who had washed her body before burial, the Scotland Yard team concluded that Bhutto died from a head injury when a powerful blast made her body hit the roof hatch of her SUV.⁶⁵ The only apparent injury was a major trauma to the right side of the head, which experts said was not an entry or exit wound from a gunshot. A British Home Office pathologist said, "The only tenable cause for the rapidly fatal head injury is that it occurred as the result of impact due to the bomb blast. Given the severity of the injury, it is impossible that she inadvertently struck her head while ducking."⁶⁶ Scotland Yard noted the escape hatch had a solid lip of four inches and Bhutto did not completely disappear from view until 0.6 seconds before the blast. However, the limited X-ray material and the absence of a full autopsy and CAT scan meant that the pathologist could not rule out the possibility of a gunshot wound to the upper trunk or neck.

Scotland Yard concluded that only one person had been involved in the attack. The team

noted that security officials found body parts from only one unidentified individual—the probable suicide bomber, according to expert opinion. Media footage placed the gunman at the rear of the vehicle and looking down immediately before the explosion. No suspicious movements by others in the crowd appeared on the footage. Forensic evidence indicated that the bomber was one to two meters from the vehicle with no obstruction in front of him, strongly suggesting that the gunman and bomber were at the same location. It is virtually impossible that anyone who was standing near the gunman who could be clearly seen on the video could have survived the blast and escaped. Scotland Yard’s final report did not discuss the possibility that vital forensic evidence could have been removed inadvertently or willingly in the post-bomb cleanup.⁶⁷

The Scotland Yard report focused primarily on the events leading up to and just after Bhutto’s assassination. Left unaddressed was the key question: Who ultimately was responsible for Bhutto’s death? Bhutto’s death had captured the world’s attention, spawning many theories about who had ordered it. The challenge is to generate a comprehensive list of suspects, identify the most diagnostic information and key information gaps, identify a robust and comprehensive set of suspects, and provide a compelling case for who were the most culpable players behind the scenes.

RECOMMENDED READINGS

Jones, Owen Bennett. *Pakistan: Eye of the Storm*. New Haven, CT: Yale University Press, 2009.
Rashid, Ahmed. *Descent into Chaos: The US and the Disaster in Pakistan, Afghanistan, and Central Asia*, paperback ed. New York: Penguin Books, 2009.

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

THE ASSASSINATION OF BENAZIR BHUTTO

Structured Analytic Techniques in Action

In this case, law enforcement and national security analysts were faced with a similar challenge: combing through large amounts of information of varying reliability to determine who ultimately was responsible for Benazir Bhutto's death. The answer to the question could have serious consequences both within Pakistan and for Pakistani relations with other countries, particularly if any Pakistani government officials were implicated in the assassination. The challenge is to sort through the data, select the most salient and defensible items of evidence, and construct a compelling story identifying the most likely culprits. The use of techniques such as Chronologies and Timelines, Mind Maps, and Analysis of Competing Hypotheses can help analysts accomplish each of these tasks.

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?
- STEP 2:** Review the Timeline by asking the following questions: Are there data gaps? Do the duration and sequence of events suggested by the data make sense? Could any events outside the Timeline have influenced the activities? Should any underlying assumptions about the evidence be taken into consideration?

Analytic Value Added. What does the sequence of events tell you? Are there any gaps in the information that should be addressed? What additional information should you seek? How confident are you in the sources of information?

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.

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.

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.

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.

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.

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.

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

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

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

Analytic Value Added. Does the creation of the Mind Map prompt you to consider a much

broader array of potential explanations or hypotheses? Does it help you “drill down” for each hypothesis to consider second- and third-level questions? Does it help you identify potential gaps in knowledge?

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.

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.

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?

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.

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.

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

STEP 9: Identify indicators or milestones for future observation.

Analytic Value Added. As a result of your analysis, what are the most and least likely hypotheses? What are the most diagnostic pieces 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?

NOTES

1. Benazir Bhutto, "When I Return to Pakistan," *Washington Post*, September 20, 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/19/AR2007091901705.xlink.html>.
2. Rubab Saleem, "Biography of PPP Chairperson Benazir Bhutto," *Pakistan Times*, December 27, 2007, <http://www.pak-times.com/2007/12/27/biography-of-ppp-chairperson-benazir-bhutto/>.
3. Fatima Bhutto, "Aunt Benazir's False Promises," *Los Angeles Times*, November 14, 2007, <http://www.latimes.com/news/printedition/asection/la-oe-bhutt014nov14,0,2985133.story>.
4. "Obituary: Benazir Bhutto," *BBC News*, December 27, 2007, http://news.bbc.co.uk/2/hi/south_asia/2228796.stm.
5. Owen Bennett Jones, *Pakistan: Eye of the Storm* (New Haven, CT: Yale University Press, 2009), 301–2.
6. Declan Walsh, "Musharraf and Bhutto Close to Sharing Power," *Guardian*, October 5, 2007, <http://www.guardian.co.uk/world/2007/oct/05/pakistan.benazirbhutto/>.
7. BBC News, "Sharif's Party 'to Contest Polls,'" December 9, 2007, http://news.bbc.co.uk/2/hi/south_asia/7135535.stm.
8. 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_15Apr12010.pdf.
9. Garhi Khuda Bakhsh, "A Country on the Brink," *Economist*, January 3, 2008, <http://www.economist.com/node/10430324/>.
10. "Huge Crowds Greet Bhutto Return," *BBC News*, October 18, 2007, <http://news.bbc.co.uk/2/hi/7050274.stm>.
11. "Two Blasts Strike Crowd Celebrating Bhutto's Return," *MSNBC*, October 19, 2007, <http://www.msnbc.msn.com/id/21344367/>.
12. Carlotta Gall and Salman Masood, "Bomb Attack Kills Scores in Pakistan as Bhutto Arrives," *New York Times*, October 18, 2007, <http://www.nytimes.com/2007/10/19/world/asia/19iht-19pakistan.7956073.xlink.html>.
13. Ahmad Rashid, *Descent into Chaos: The US and the Disaster in Pakistan, Afghanistan, and Central Asia* (New York: Penguin Books, 2009), 379.
14. "Two Blasts Strike Crowd."
15. Jones, *Pakistan*, 4.
16. Pakistan People's Party, "Bhutto Names Suspects in Letter to Musharraf," October 24, 2007, <http://www.ppp.org.pk/mbb/articles/article121.xlink.html>.
17. Philip Sherwell, "Bhutto 'Blocked from Hiring US Bodyguards,'" *Sunday Daily Telegraph*, December 30, 2007, <http://www.telegraph.co.uk/news/worldnews/1574054/Bhutto-blocked-from-hiring-US-bodyguards.html>.
18. Gail Sheehy, "A Wrong Must Be Righted: An Interview with Benazir Bhutto," *Parade*, January 6, 2008, http://www.parade.com/articles/editions/2008/edition_01-06-2008/Benazir_bhuttoTest/.
19. Bhutto, "Aunt Benazir's False Promises."
20. Carlotta Gall and Salman Masood, "After Bombing, Bhutto Assails Officials' Ties," *New York Times*, October 20, 2007, <http://www.nytimes.com/2007/10/20/world/asia/20Pakistan.html>.
21. Zahid Hussain, "Musharraf and Bhutto in Power-Sharing Talks," *Times* (London), July 28, 2007, <http://www.timesonline.co.uk/tol/news/world/asia/article2155462.ece>.
22. Carlotta Gall, "Bhutto's Return Brings Pakistani Politics to a Boil," *New York Times*, October 30, 2007, <http://www.nytimes.com/2007/10/30/world/asia/30pakistan.html>.
23. Jemina Klan, "A Kleptocrat in a Hermès Scarf," *Daily Telegraph*, October 21, 2007, <http://www.telegraph.co.uk/comment/3643479/Benazir-Bhutto-a-kleptocrat-in-a-Hermes-scarf.html>.
24. Imran Khan, "Benazir Bhutto Has Only Herself to Blame," *Daily Telegraph* (UK), October 21, 2007, <http://www.telegraph.co.uk/comment/3643478/Benazir-Bhutto-has-only-herself-to-blame.html>.
25. Gall, "Bhutto's Return Brings Pakistani Politics to a Boil."
26. Ibid.
27. BBC News, "Ex-PM Bhutto under House Arrest," November 9, 2007, <http://news.bbc.co.uk/2/hi/7086272.stm>.
28. Bhutto, "Aunt Benazir's False Promises."
29. Benazir Bhutto, "Benazir Bhutto's Letter to Peter Galbraith," *CHOWK*, November 14, 2007, <http://www.chowk.com/ayesha5/iLogs/life/Benazir-Bhutto-s-letter-to-PeterGalbraith/>.
30. Griff Witte and Emily Wax, "Bhutto's Last Day, in Keeping with Her Driven Life," *Washington Post*, January 16, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/15/AR2008011503304.xlink.html>.
31. Ali Hazrat Bacha, "Youth with Dynamite Held Near Rally Venue," *Dawn*, December 27, 2007, <http://www.dawn.com/2007/12/27/top8.htm>.

32. Witte and Wax, "Bhutto's Last Day."
33. Saeed Shah and Andrew Buncombe, "Bhutto Had 'Proof' of Plan to Rig Election," *Independent* (UK), January 1, 2008, <http://www.independent.co.uk/news/world/asia/bhutto-had-proof-of-plan-to-rig-election-767540.xlink.html>.
34. Associated Press, "In Meeting with Karzai, Bhutto Wanted Peace, Democracy for Afghanistan and Pakistan," December 27, 2007, <http://www.afghanistannewscenter.com/news/2007/december/dec282007.xlink.html#3>.
35. Witte and Wax, "Bhutto's Last Day."
36. Kamran Haider, "Four Dead in Pakistan Election Shooting," Reuters, December 27, 2007, <http://in.reuters.com/article/article/2007/12/27/idINIndia-31134720071227/>.
37. Witte and Wax, "Bhutto's Last Day."
38. United Nations, *Report of the Assassination of Mohtarma Benazir Bhutto*.
39. Ibid.
40. CNN, "Pakistan: Fractured Skull Killed Bhutto," December 28, 2007, <http://www.cnn.com/2007/WORLD/asiapcf/12/28/pakistan.friday/index.html>.
41. CNN, "Ministry Backtracks on Bhutto Sunroof Claims," January 1, 2008, <http://www.cnn.com/2008/WORLD/asiapcf/01/01/pakistan.autopsy/index.html>.
42. Ibid.
43. United Nations, *Report of the Assassination of Mohtarma Benazir Bhutto*.
44. Ibid.
45. CNN, "Ministry Backtracks on Bhutto Sunroof Claims."
46. Aryn Baker and Simon Robinson, "Missing Evidence from Bhutto's Murder," *Time*, December 31, 2007, <http://www.time.com/time/world/article/0,8599,1699138,00.xlink.html>.
47. Simon Robinson, "Bhutto Conspiracy Theories Fill the Air," *Time*, December 28, 2007, <http://www.time.com/time/world/article/0,8599,1698828,00.xlink.html>.
48. United Nations, *Report of the Assassination of Mohtarma Benazir Bhutto*.
49. Carlotta Gall, "Musharraf Denies Link to Attack on Bhutto," *New York Times*, January 3, 2008, <http://www.nytimes.com/2008/01/03/world/asia/03iht-pakistan.4.9012655.xlink.html>.
50. Ibid.
51. Ibid.
52. CNN, "Musharraf Denies Bhutto Death Role," January 4, 2008, <http://www.cnn.com/2008/WORLD/asiapcf/01/03/pakistan.elections/index.html>.
53. Jones, *Pakistan*, 5–6.
54. Joby Warrick, "CIA Places Blame for Bhutto Assassination," *Washington Post*, January 18, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/17/AR2008011703252.xlink.html>.
55. Paul Cruickshank, "Hunting Bhutto's Killer," *Guardian*, January 1, 2008, <http://www.guardian.co.uk/commentisfree/2008/jan/01/huntingbhuttoskiller/>.
56. *The Nation* (Pakistan), February 8, 2005, cited in Sohail Abdul Nasir, "Baitullah Mehsud: South Waziristan's Unofficial Amir," *Terrorism Focus* 3, no. 26 (2006), http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=829.
57. Afzal Khan, "Baitullah Mehsud: Scapegoat or Perpetrator in Benazir Bhutto's Assassination?" *Terrorism Monitor* 6, no. 5 (2008), [http://www.jamestown.org/programs/gta/single/?tx_ttnews\[tt_news\]=4775&tx_ttnews\[backPid\]=167&no_cache=1](http://www.jamestown.org/programs/gta/single/?tx_ttnews[tt_news]=4775&tx_ttnews[backPid]=167&no_cache=1).
58. *The Nation*, n.d., cited in "Who Is Aitezaz Shah?" *Pakistani Spectator*, February 2, 2008, <http://www.pkhope.com/who-is-aitezaz-shah/>.
59. " 'Bhutto Murder Suspect' Arrested," Al Jazeera, January 19, 2008, <http://english.aljazeera.net/news/asia/2008/01/2008525125158691764.xlink.html>.
60. "Teenager Suspect Arrested in Bhutto Assassination," *Economic Times* (India), January 20, 2008, <http://economictimes.indiatimes.com/teenager-suspect-arrested-in-bhutto-assassination/articleshow/2714625.cms>.
61. Farhan Bokhari, "PPP Pushes for Independent Bhutto Probe," *Financial Times*, January 20, 2008, <http://www.ft.com/cms/s/0/333552c6-c774-11dc-a0b4-0000779fd2ac.html#axzz1PAbsOkON>.
62. Jones, *Pakistan*, 4.
63. Scotland Yard, "Scotland Yard Report on Assassination of Benazir Bhutto," *Hindu* (India), February 9, 2008, <http://www.hindu.com/2008/02/09/stories/2008020960750101.htm>.
64. Alisha Haider, "Scotland Yard Investigation Is Useless," *Washington Post*, February 14, 2008, http://onfaith.washingtonpost.com/postglobal/needtoknow/2008/02/scotland_yard_investigation_pu.html.
65. Scotland Yard, "Report on Assassination of Benazir Bhutto."
66. Ibid.
67. Ibid.

9 Death in the Southwest

Key Questions

- ▶ What caused a presumably healthy young Navajo couple to die suddenly?
- ▶ What initial assumptions were made about the cause of death?
- ▶ What alternative explanations should be considered?
- ▶ What information would best help identify the cause of death?

CASE NARRATIVE

On 14 May 1993 in the Four Corners area of New Mexico, a young former track star collapsed on the way to his fiancée's funeral and was rushed to the Gallup Medical Center emergency room. He died a few hours later. State medical investigators performed autopsies on both the man and his fiancée, who had died five days earlier. They noted similarities in their cases: flu-like symptoms of fever, coughing, and chills, with quick progression to acute respiratory distress and death as their lungs filled with fluid. Their infant daughter also exhibited the same symptoms but was not as severely affected.¹ None of the medical personnel involved in treating the patients were believed to have become infected.

Three days later, Gallup Medical Center officials linked the deaths of the young couple to three other respiratory fatalities in the region and sent a warning to the New Mexico Department of Health. Doctors were concerned that they were dealing with a particularly potent flu virus that could spread quickly across the broader population. The next day the Department of Health contacted the federal Centers for Disease Control (CDC) in Atlanta, Georgia, and asked it to investigate.²

By 31 May 1993, the disease had claimed ten victims, eight of them Navajos. Young, healthy adults were dying of an infectious disease that appeared to have a surprisingly high case-fatality rate.³ An epidemiologist from the New Mexico Department of Health reported that all died shortly after developing symptoms similar to the flu, including a cough that quickly progressed to a severe respiratory ailment. The official said that the department did not know what the illness was or how to prevent it; initial laboratory polymerase chain reaction (PCR) tests for common viral and bacterial agents had come back negative.⁴

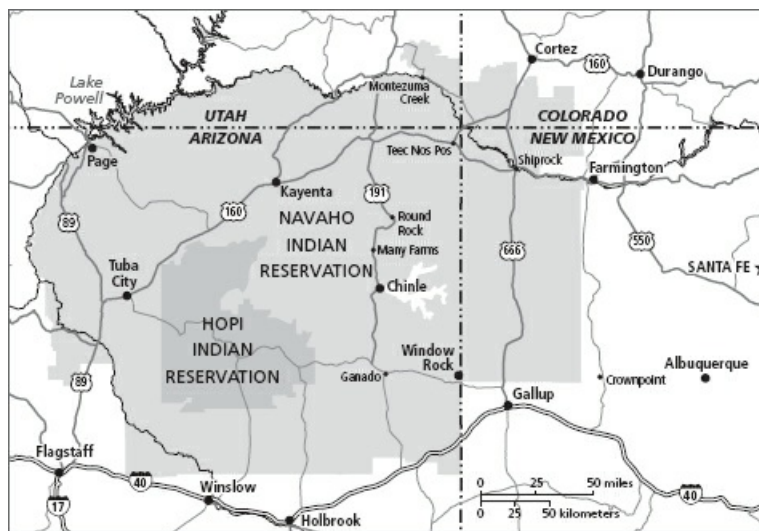
Medical officials realized they were facing a major challenge: people were dying, and no one knew why. Were all these deaths related? If so, what common symptoms could be identified? Doctors were concerned that if they could not determine the underlying cause of death, they could not treat those who were becoming ill and they could not prevent even more people from

dying.

The Four Corners Region

Four Corners (see Map 9.1) is a region of the United States that encompasses southwest Colorado, northwest New Mexico, northeast Arizona, and southeast Utah. The name comes from a monument that marks the only spot in the United States where the boundaries of four states intersect. The monument also denotes the boundary between two semi-autonomous Native American governments, the Navajo Nation, which maintains the monument as a tourist attraction, and the Ute Mountain Ute Indian Reservation.⁵

Map 9.1 ► Four Corners Region



Many residents of the Four Corners region depend on tourism and agriculture for their livelihoods. The area hosts thousands of visitors yearly who come to the region to visit Canyon de Chelly National Monument and Mesa Verde National Park, which contain ruins of early indigenous tribes, and Monument Valley, which is notable for its large sandstone buttes. Other residents earn their livelihoods from livestock farming, seasonal migratory agricultural work, and employment off the Navajo reservation.⁶

The Four Corners Region is a high plateau: weather systems stabilize here and then head eastward to create snow and rain in the central portion of the United States. The area itself has low humidity, sparse precipitation, and lots of sun. The winters are mild during the day, with temperatures falling to or below freezing at nightfall. When El Niño occurs, usually every three to seven years, the winters and early springs tend to be wetter than usual. Stronger than usual El Niños bring significantly more rainy days and more rain per day. Summers are hot. Forty percent of the region's precipitation comes from late-afternoon summer thunderstorms. Water rights and access to water are important issues in the area.⁷

The Navajo Nation constitutes the bulk of the population in the Four Corners region. The Nation's reservation encompasses more than twenty-seven-thousand square miles, with three satellite locations in central New Mexico. The Navajo are inheritors of a cultural legacy centered on oral traditions and customs passed down for hundreds of years. The tribe's spiritual beliefs,

collectively known as the Navajo Way, emphasize the importance of preserving and restoring balance and harmony with nature. According to cultural specialists at the Navajo Nation Museum in Window Rock, Arizona, sacred ceremonies performed by tribal healers are essential in perpetuating the Navajo Way. The Navajo medicine people (*hataa'lii* in the Navajo language) serve not only as healers but as historians with extensive knowledge of tribal traditions and mythology.⁸

The Navajo Area Indian Health Service (NAIHS), a subagency of the Department of Health and Human Services, is responsible for health care for American Indians in the Four Corners area; its primary patients are members of the Navajo Nation and the Southern Band of San Juan Paiutes, but NAIHS also provides care to other Native Americans. All NAIHS physicians must be board eligible or, preferably, board certified in a Western medical specialty. The NAIHS sensitizes its medical professionals to the intertwining of Navajo religion with the concepts of being, health, disease, and the environment. The Navajo Nation Council's Division of Health Improvement Services—later renamed the Navajo Division of Health—also plays a role in promoting and maintaining the overall health and well-being of the Navajo population. It employs hundreds of health professionals, paraprofessionals, and technical professionals scattered throughout the Navajo Nation.⁹

Fear Takes Over

By the end of May, at least twenty-three patients—predominantly Navajos—with symptoms of the illness were being treated at hospitals in the Four Corners area and Albuquerque, New Mexico. Communicable disease specialists from the Indian Health Service in Albuquerque said that they had not yet been able to determine why people who were closely related to each other (family cluster cases) developed adult respiratory distress syndrome in roughly the same time period. In all cases, the disease—which some labeled the “Navajo flu”—progressed quickly, though it did not always lead to death. Press reports stated that four people appeared to have recovered, but doctors said they did not know whether treatment, primarily with antibiotics, was responsible.¹⁰

As news of the illness spread across the country, tourism to the Four Corners area declined. Twenty-seven young Navajos who corresponded with students at a private school in the Los Angeles area were discouraged from visiting their pen pals. Special telephone lines set up by the New Mexico Department of Health to handle inquiries about the illness were overwhelmed with calls. Hospitals in Santa Fe began seeing panicky patients who had visited the Navajo reservation within the past several weeks. Following the discovery of “new” and “unknown” diseases, it is typical behavior for a sensitized population within the presumably affected community to respond by inundating the available medical infrastructure.¹¹

In Atlanta, three young investigators in the Centers for Disease Control's Epidemic Intelligence Service (EIS) were called on a Friday afternoon in late May and told to come to the office.¹² They were handed airline tickets and gas masks, the latter suggesting the possibility that they could be exposed to a toxic substance. The EIS, the “special pathogens” branch of the CDC, is primarily deployed when a new pathogen is discovered or if there is an allegation or suspicion of bioterrorism. The service was created in 1951 during the Korean War, when the United States became worried about biological warfare. A preliminary survey of the Internet, however, revealed no postings containing extreme anti-Navajo rhetoric or any suggestions that terrorists might be targeting the Four Corners area.

The connection with bioterrorism was not farfetched in the case of the “Navajo flu.” Some residents of the reservation speculated that victims had been exposed to a toxin stored at Fort Wingate Army Depot, a munitions storage and demolition facility close to both the Navajo Nation and the Zuni Pueblo Tribe. Others asked whether there were any reports of toxic spills on or near Navajo Nation lands.¹³

Collecting the Pieces of the Puzzle

The EIS epidemiologists were skeptical that they were dealing with a flu virus. They were working against the clock to determine not only the type of illness but its root cause. EIS personnel began working with a small group of investigators assembled from the state health departments, the University of New Mexico School of Medicine, and the Navajo Area Indian Health Service. They began combing through patient logs made available by area hospitals and clinics.

Their research revealed that most patients lived in the Four Corners area, but the available data did not show the victims all visiting the same location or any obvious patterns. Most patients reported influenza-like symptoms of abrupt fever, nausea, vomiting, headache, malaise, and body aches—particularly abdominal and back pain. This was often followed by a cough, gastrointestinal manifestations, and labored breathing for four or more days before hospitalization with pulmonary edema or fluid in the lungs, along with severe hypertension and oxygen deficit in body tissues. Blood tests, when conducted, also showed abnormally low blood platelet counts, which are often associated with diseases such as rickets, the plague, rabbit fever, and deer fly fever.¹⁴ Initially, moderate cases of the illness were diagnosed as acute respiratory distress syndrome, juvenile diabetes, and even gastroenteritis. Those treating the patients did not seem to be contracting the illness.¹⁵

The investigators cast a wide investigatory net. Many of the pieces or clues were consistent with exposure to toxic material—either accidental or on purpose: presence of an unexplained disease in a discrete population, many cases of death from an unexplained disease, a disease that is unusual for an age group, a disease that is much more severe than expected, the failure to respond to standard therapy, and the presence of munitions or advanced weapons delivery systems.¹⁶ A few patients reported dizziness, confusion, or impaired concentration, all of which are symptoms of exposure to toxic material. If a biological agent were being used deliberately to cause the deaths, one sign would be a high number of recent, unexplained animal deaths or crop failures, but research did not turn up any such evidence.

EIS personnel also sought out Navajo tribal healers, who were the closest thing to a historical medical registry available. The healers told EIS personnel that the cause of the disease was disharmony in the Navajo world. They recounted that many people had died of sudden, powerful diseases two other times during the twentieth century, in 1918 and 1933. Tribal elders recalled that there were particularly abundant piñon, or pine nut, crops those years because of unusually wet winters and springs. According to tribal lore, rodent populations were also very high during those times.¹⁷

Rodents are well known as potential carriers of disease. Investigators asked: Was the outbreak of a similar virus and the increase in rodent populations on two other occasions earlier in the century a coincidence, or did the correlation suggest the source of the disease? Investigators needed to know as soon as possible what kinds of illnesses rodents are known to spread and whether such illnesses were endemic to the Four Corners region. Preliminary research

suggested some answers, as shown in Table 9.1.

Table 9.1 ▶ Diseases Transmitted by Rodents

Diseases Directly Transmitted by Rodents	Geographic Region Where Disease Occurs
Rat-bite fever	Worldwide; endemic to Four Corners area
Leptospirosis	Worldwide; endemic to Four Corners area
Salmonellosis	Worldwide; endemic to Four Corners area
Lymphocytic choriomeningitis virus	Worldwide
Rabies	Rodent-spread case in Florida in 1980
Plague	Western United States, South America, Africa, and Asia

The investigators reached out to climatologists as well. The climatologists confirmed that precipitation levels had increased dramatically in 1992 and 1993 in association with El Niño. The rainfall resulted in an abundance of vegetation and ample food supplies for rodent populations. When precipitation levels returned to normal, however, rodent populations became stressed due to the lack of food supply, forcing them to seek new sources of food. The National Science Foundation and the US Fish and Wildlife Service recommended that medical investigators consult scientists associated with the Sevilleta Long-Term Ecological Research Program at the Sevilleta National Wildlife Refuge in central New Mexico. Ecological researchers provided a detailed analysis of twenty-two rodent species in the area. In reviewing the reports, the investigators were struck by the fact that there had been a tenfold increase in the rodent population between 1992 and 1993.¹⁸

People were getting sick, and many were dying, as investigators continued to collect the various pieces of the puzzle. Doctors felt a growing sense of urgency to discover the underlying cause of death. Public concern was mounting, and people deserved an explanation. More important, the public was demanding guidance on what to do to avoid getting sick, and public health officials didn't know what to say.

RECOMMENDED READINGS

Dworkin, Mark S. *Outbreak Investigations around the World: Case Studies in Infectious Disease Field Epidemiology*. Sudbury, MA: Jones and Bartlett, 2009.

Locke, Raymond Friday. *The Book of the Navajo*. Los Angeles: Holloway House, 1991.

McKenna, Maryn. *Beating Back the Devil*. New York: Free Press, 2008.

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

DEATH IN THE SOUTHWEST

Structured Analytic Techniques in Action

In a crisis situation, analysts are often forced to make difficult judgments with little solid data in hand. The following techniques and exercises can be used to tackle these types of situations by using Structured Brainstorming to think creatively and exhaustively, Starbursting to organize that thinking around key questions, the Multiple Hypotheses Generator™ to generate a full range of alternative hypotheses, and a Key Assumptions Check and Analysis of Competing Hypotheses (ACH) to scrutinize the evidence.

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.

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

speaking.

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).

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.

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.

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?

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.

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.

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.
- 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. Can you identify four or five key factors or forces that might explain why the young Navajo couple died?
- STEP 12:** Present the results, describing the key themes or dimensions of the problem that deserve investigation.

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? 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?

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 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.
- 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 deserve further investigation?

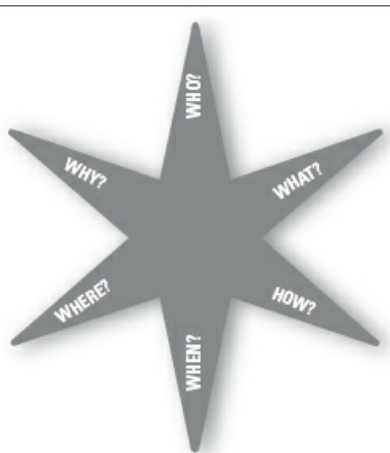
Technique 3: Key Assumptions Check

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.

Figure 9.1 ▶ Starbursting Template



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.

Table 9.3 ▶ Key Assumptions Check Template

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

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.

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.

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

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?

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?

STEPS 2 AND 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.

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

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.

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

STEP 8: Restate the permutations 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.

Analytic Value Added. Which hypotheses should be explored further? Which of the six key components (Who? What? How? When? Where? and Why?) can be set aside because they are “givens,” and why? Which hypotheses from the original list were discarded, and why?

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.
- 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 consistent, consistent, highly inconsistent, inconsistent, neutral, or not applicable 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.
- 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?
- 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.
- STEP 7:** 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.
- STEP 8:** Report the conclusions by considering the relative likelihood of all the hypotheses.
- STEP 9:** Identify indicators or milestones for future observation.

Analytic Value Added. As a result of your analysis, what are the most and least likely hypotheses? What are the most diagnostic pieces 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 hypotheses?

NOTES

1. “Mystery Illness Takes 10th Life in the Southwest,” *New York Times*, May 31, 1993, <http://www.nytimes.com/1993/05/31/us/mystery-illness-takes-10th-life-in-the-southwest.html>.
2. Ecological Society of America, *Ecological Research Benefits: The Hantavirus Case Study*, August 25, 2009, http://www.esa.org/education_diversity/pdfDocs/hantavirus.pdf.
3. C. J. Peters and Ali S. Khan, “Hantavirus 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>.
4. “Mystery Illness Takes 10th Life in the Southwest.”
5. Rick Abasta, “Four Corners Monument Still the Legally Recognized Landmark Despite Reports,” Navajo Nation Parks & Recreation Department, http://navajonationparks.org/pr/pr_4Cmarker.htm; US Department of Energy, “Ute Mountain Ute Indian Reservation—General Setting,” http://www1.eere.energy.gov/tribalenergy/guide/pdfs/ute_mountain_ute.pdf.

6. Robert S. McPherson, "Navajo Indians," http://www.historytogo.utah.gov/utah_chapters/american_indians/navajoindians.html; US Department of Energy, "Ute Mountain Indian Reservation"; Indian Country Extensions, "Navajo Nation—Shiprock."
7. Tripcart.com, "Weather in Four Corners of New Mexico, Arizona, Utah, and Colorado," <http://www.tripcart.com/usa-regions/Four-Corners/Weather.aspx>; Kathleen Ward, "Rainmaker Go North—Nebraska Needs Help, Too," October 10, 2002, http://www.ksre.ksu.edu/news/sty/2002/weather_winter101002.htm; Western Regional Climate Center, "El Niño, La Niña, and the Western US, Alaska, and Hawaii," compiled by Kelly Redmond, updated June 26, 1998, <http://www.wrcc.dri.edu/enso/ensofaq.html>.
8. Lauren Monsen, "Navajo Healers, Sand Paintings Keep Tribal Traditions Alive," NewsBlaze.com, n.d., <http://newsblaze.com/story/20080920133834tsop.nb/topstory.html>; Navajo Nation Government, "History," <http://www.navajo.org/history.htm>.
9. Indian Health Service, "Navajo Area Office: Navajo Area Jobs and Recruitment," http://www.ihs.gov/navajo/index.cfm?module=najr_main; Indian Health Service, "Cross Culture Medicine," http://www.ihs.gov/Navajo/index.cfm?module=nao_cross_culture_medicine.
10. "Mystery Illness Takes 10th Life in the Southwest."
11. "Four Corners," Wikipedia, http://en.wikipedia.org/wiki/Four_Corners_region; Jill Leovy and Jack Cheevers, "Visiting Navajo Children Barred from L.A. School," *Los Angeles Times*, June 2, 1993, http://articles.latimes.com/1993-06-02/news/mn-42529_1_navajo-children/; Maureen Trudelle Schwarz, *Navajo Lifeways: Contemporary Issues, Ancient Knowledge* (Norman: University of Oklahoma Press, 2001), 23.
12. Tom Paulson, "Doctor on Trail of Another Deadly Virus," *Seattle Post-Intelligencer*, April 10, 2003, http://www.seattlepi.com/local/116784_outbreak10.html.
13. Ibid.
14. Peters and Khan, "Hantavirus Pulmonary Syndrome."
15. Lone Simonsen, Mary J. Dalton, Robert F. Brieman, Thomas Hennessy, Edith T. Umland, C. Mack Sewell, Pierre E. Rollin, Thomas G. Ksiazek, and Clarence J. Peters, "Evaluation of the Magnitude of the 1993 Hantavirus Outbreak in the Southwestern United States," *Journal of Infectious Diseases* 172, no. 3 (1995): 729–33; John H. Grendon and Marcia J. Goldoft, "Discovery of Hantavirus Syndrome in Washington State," *Washington Public Health* 14 (1996), <http://www.nwpublichealth.org/docs/wph/hanta.html>; Peters and Khan, "Hanta Pulmonary Syndrome."
16. Robert G. Darling and Jon B. Woods, eds., *USAMRIID's Medical Management of Biological Casualties Handbook*, 5th ed. (Frederick, MD: US Army Medical Research Institute of Infectious Diseases, 2004), <http://www.usamriid.army.mil/education/bluebookpdf/USAMRIID%20Blue%20Book%205th%20Edition.pdf>.
17. 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>.
18. Ecological Society of America, *Ecological Research Benefits: The Hantavirus Case Study*.

10 The Atlanta Olympics Bombing

Key Questions

- ▶ Who was responsible for placing the bomb in Centennial Park?
- ▶ What were the most critical pieces of evidence in this case?
- ▶ Who was the federal authorities' prime suspect, and why?

CASE NARRATIVE

Carnage in Centennial Park

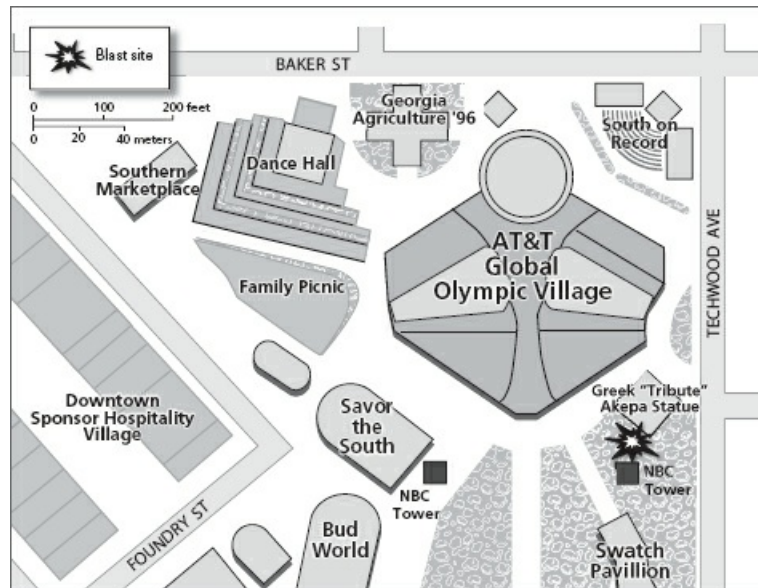
In the summer of 1996, world attention focused on Atlanta, Georgia, as the city proudly hosted the Centennial Olympic Games. With some fifteen thousand athletes from 197 countries competing and millions of spectators in attendance, state, local, and federal authorities invested a great deal of resources on site security. In all, officials spent an estimated \$227 million on security to deploy about thirty thousand police, military, and private guards, as well as an array of high-technology equipment.¹ Authorities described the effort as the largest peacetime security operation for a public event in American history.²

Beginning three months before the Olympics opening ceremony, the Atlanta Olympic Committee transformed a twenty-one-acre site from an unused area of slums and old warehouses into Centennial Park—a popular entertainment venue for those attending the games (see Map 10.1).³ The park attracted some hundred thousand people a day to relax and party on the outskirts of the Olympics. On 26 July 1996, the ninth day of the Olympics, authorities estimated that forty thousand to fifty thousand people gathered in the park to attend a Friday night concert.⁴ At 0120, Jack Mack and the Heart Attack were performing on stage at the AT&T Pavilion when a bomb exploded, spreading nails and shrapnel through a portion of the crowd. The blast killed Alice Hawthorne, who had brought her daughter to the Olympics as an early birthday present, and injured 111 others.⁵ A Turkish cameraman, Melih Uzunyol, died of a heart attack responding to the blast.⁶ Hopes for holding an Olympics without a terrorist incident were shattered.

Eyewitnesses described a scene of horror and carnage at the park, with wounded people everywhere.⁷ Police officers reported people on the ground screaming. When the smoke cleared, six state troopers and one Georgia State Bureau of Investigation agent were among those injured in the blast.⁸ One thirty-three-year-old officer reported, “I saw the flash. I saw the puff of smoke. I saw the orange flame. Then something grabbed me and threw me across the ground.”⁹ A nearby press center was closed immediately because guards feared another explosion. Richard Jewell, a security guard, was proclaimed a hero for spotting a suspicious knapsack, alerting

authorities, and helping them clear the area prior to the explosion. Nine police officers were also involved in trying to clear the area before the bomb went off, and all were credited with having substantially reduced the number of casualties from the explosion.

Map 10.1 ► Centennial Park



Atlanta chief of police Beverly Harvard noted that they had been receiving bomb threats on a regular basis prior to the incident and were concerned about the potential for copycat bombings in the wake of the Centennial Park bombing. Bomb threats continued over the weekend. Law enforcement officials ordered the evacuation of a shopping center, two subway stations, a bank, and a church because of bomb threats as they worked quickly to identify those responsible for the bombing.¹⁰

The Broader Context

Local law enforcement officials as well as the Federal Bureau of Investigation (FBI) had been concerned for some time about the possibility of a terrorist attack against the Olympic Games. Just days before the opening ceremonies on 17 July 1996, TWA Flight 800 had taken off from New York's Kennedy Airport and exploded in midair over Long Island Sound, killing 228 passengers.¹¹ The reason for the crash was still being investigated, but a terrorist attack was a distinct possibility. Security concerns in Atlanta were underscored when a man carrying a loaded handgun sneaked into Olympic Stadium before the opening ceremony. The man was dressed as a security guard and was arrested; police later released him after deciding that he did not pose a threat.¹² Just three months earlier in April 1996, members of a militia group had been arrested in central Georgia and accused of conspiring to stockpile bombs for a "war" with the government.¹³

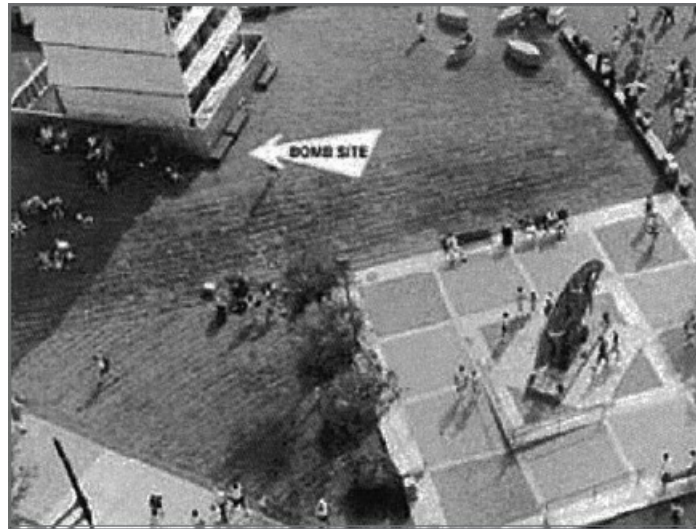
Law enforcement officials also remembered that the Palestinian terrorist organization known as Black September had struck at the 1972 Olympics in Munich. In that attack, the Palestinians took eleven Israeli athletes hostage for twenty-three hours in the hope of attracting attention to the Palestinian cause and forcing the Israeli government to free 242 political prisoners from jail. The crisis culminated in a deadly shootout on an airport tarmac that ended with the deaths of one

German police officer and all eleven Israeli hostages.¹⁴

Since then, governments hosting the Olympic Games have devoted considerable resources to ensuring that the games would not be stained by another terrorist attack. Billions had been spent by governments around the world since 1972 to keep the games safe, and Atlanta authorities had taken the threat of a terrorist attack seriously.¹⁵

The Investigation

Just prior to the explosion, Tom Davis, a Georgia Bureau of Investigation agent, went to Centennial Park on a routine call to handle a few overexcited revelers attending a concert.¹⁶ When he arrived at the park, the rowdies apparently had already departed, but a stage security guard, Richard Jewell, caught his attention. Jewell was one of a handful of contract guards retained by AT&T after it had canceled a previous contract with another security company two weeks earlier.¹⁷



FBI photo of green bench in front of NBC's sound tower.

Jewell showed Davis a suspicious package—a green knapsack that had been left unattended under a green bench at the foot of a huge NBC media sound and light tower that had been built to support the stage shows. Davis immediately called a bomb diagnostic team and, as other officers joined him, started ushering people away from the site of the abandoned knapsack.

Jewell later said that he routinely made security sweeps around the tower, checking under benches and making sure nothing was amiss. He said he was certain the knapsack was not in the area at 2130, but he did notice it on his next check around 0050 after the rowdy group had departed.¹⁸ He suspected the rowdy group had left the knapsack behind. Davis checked with some revelers in the area, and they said it was not their knapsack. Davis and Jewell asked several others if they knew whose knapsack it was, but no one claimed ownership.¹⁹

Jewell told investigators he was forty feet away when the bomb exploded, but the impact still knocked him off his feet. When he looked up, he saw two Georgia state troopers sailing through the air.²⁰

The FBI Takes Command

The FBI took the lead in the investigation.²¹ At a press conference held on 29 July, FBI spokesperson David Tubbs noted that numerous law enforcement agencies were involved and that they had received a substantial number of leads that they were tracking down. He cautioned the press that it was important not to draw any conclusions from questions that were being asked and said the Bureau had not identified a suspect. He indicated that the Bureau was focusing on domestic rather than international terrorism.

Law enforcement officials said the list of possible bombers ranged from antigovernment militia members to disgruntled employees.²² Investigators speculated early in the investigation that an extremist militia-type group or an organization that was anti-government could be behind the bombing.²³ Based on one of the composite sketches made after the bombing, FBI agents interviewed an Alabama militia member, but then ruled him out as a possible suspect. Other potentially violent domestic extremist groups such as white supremacists, sovereign citizens, and anti-abortion groups also merited attention. The Bureau expanded its search to consider disgruntled AT&T employees because the bomb site was next to an AT&T facility from which people recently had been dismissed. FBI Director Louis Freeh would later say that the Bureau had identified “several suspects” early on in the case, but all suspects “washed out” after law enforcement discovered evidence that was exculpatory or inconsistent with investigating the individuals further.²⁴

Tubbs told the press that a 911 call was made at approximately 0100 from a pay phone outside the downtown Days Inn. The next day, the FBI released the exact wording of the warning call: “There is a bomb in Centennial Park. You have thirty minutes.” The FBI spokesperson said the Bureau believed the voice was that of a “white American made with an indistinguishable accent.”²⁵

The 911 police log obtained by the Associated Press (AP) lists three entries logged into the Atlanta police 911 computer early in the morning of 27 July.²⁶

- ▶ 00:55:35, apparently the time the call was received. According to the dispatcher’s notes, the caller was “very calm and even” and sounded like a white man.
- ▶ 01:08:35, followed by an abbreviation “DIS,” apparently referring to the dispatch of one or more officers.
- ▶ 01:12:52, followed by “ARV,” apparently referring to an officer arriving at an unspecified location.

Terrorism experts and Fulton County sheriff Jacquelyn H. Babbett said the 911 warning may have been an attempt to lure police and security officers to the site of the bombing to injure them.²⁷ According to one terrorism expert, the phone warning was a classic ambush technique designed to clear an area of civilians but draw police to the scene to kill them. The placement of nails around the bomb showed that the intent was not just to have a big bang but to kill people.²⁸ A retired Bureau of Alcohol, Tobacco, and Firearms official, Robert Holland, said in an interview that when a bomber says people have thirty minutes and the bomb goes off eighteen minutes later, there is a good possibility the bomber intended to take out the security forces.²⁹

The bomb itself was crudely made (see Figure 10.1). Law enforcement officials described it as a pipe bomb that used a simple clock and low-grade, easily available explosive powder. The

shrapnel that wounded so many people included masonry nails placed in a plastic food container around the explosives.³⁰ Investigators found several remnants of the bomb, including residue from a portion of the bomb that failed to explode, and shrapnel. An intact end cap from one of the three pipe bombs that were tied together to cause the blast was found by a tourist, who later turned it over to the FBI. The masonry nails had a round top, slight spiral ribs, and a very slight thread. Sources told AP that this was an odd choice of nails for a person to buy—suggesting to them that the bomber had used whatever was lying around at the time.³¹

Investigators had the telephone from which the 911 call was made and videotapes and other materials from the scene, which they hoped would lead them to a quick arrest.³² The knapsack was identified as an olive green, military-style backpack commonly known as a medium-sized ALICE pack. It had an improvised handle made by inserting a round wooden rod at the top of the pack. Investigators said that military personnel are known to have modified packs in this way and to have taught the same technique.³³

FBI investigators began interviewing large numbers of people who were present at the time of the explosion in search of more leads. They also screened videotape shot by sophisticated night-vision surveillance cameras, called SpeedDomes, that were mounted in Centennial Park and camouflaged to look like light poles.³⁴ The cameras rotate 360 degrees and have the ability to zoom in on an object of interest and magnify the image ten times. There were hundreds of SpeedDomes across the Olympic venue.

Figure 10.1 ► Bomb Specifications and ALICE Pack



The bomb in the ALICE pack consisted of three metal pipes 2 inches in diameter and 12 inches long, threaded on each end with 2-inch metal endcaps on each pipe. The bomb used three to four pounds of Accurate Arms brand #7 or #9 smokeless gunpowder. It contained about six pounds of 8d, 2 1/2-inch-long masonry nails. It used a blue, Eveready 12-volt battery; a Westclox brand “Big Ben” wind-up alarm clock; gray duct tape; and black plastic electrical tape.

Sources: FBI National Press Office, “Statement of FBI SAC Jack A. Doulton and Inspector Woody R. Enderson [press release],” November 18, 1997, <http://web.archive.org/web/20000303015458/www.fbi.gov/majcases/rudolph/presre11.htm>; Federal Bureau of Investigation, Counterterrorism Division, Counterterrorism Threat Assessment and Warning Unit, National Security Division, “Terrorism in the United States: 1996,” 1996, <http://www.fbi.gov/stats->

Jewell was interviewed by the Secret Service, the Georgia Bureau of Investigation, and the FBI on 27 July and again on 28 July. In these interviews, interrogators considered him a witness, not a suspect.³⁵ The views of investigators began to change, however, on the afternoon of 28 July following the second interview. The president of Piedmont College, Ray Cleere, called the FBI field office in Atlanta that afternoon after seeing Jewell on television to suggest that the FBI consider the possibility that Jewell had planted the bomb. Cleere noted that Jewell had had problems earlier working as a police officer at Piedmont College, and Cleere's theory was that Jewell had intentionally placed the bomb because he wanted credit for having mitigated the amount of damage done by the bomb. After doing some preliminary research, FBI agents found a case in southern California not long before the Atlanta bombing when a volunteer firefighter had apparently set a series of fires so that he could extinguish them and become a hero.³⁶

Later in the afternoon on 28 July, when the tip was passed to FBI officials in Washington during a conference call, someone on the call mentioned that a security guard at the 1984 Olympic Games in Los Angeles had planted a bomb on a bus so that he could discover it later and be a hero. FBI headquarters agreed that it was logical to conduct a preliminary investigation of Jewell's background, but the investigators focused most of their attention on other suspects.³⁷

The FBI's background investigation uncovered some interesting information. For starters, Jewell had been arrested in 1990 for impersonating a police officer. He also had work-related problems while serving as a deputy sheriff in Habersham County, Georgia.

The next day, the FBI's profiling unit said that Jewell "fit the profile of a person who might create an incident so he could emerge as a hero."³⁸ After reviewing videotape of interviews with Jewell, the profiling team said that Jewell's "account of the bombing seemed vague on important points and that he seemed uncomfortable discussing the victims."³⁹ An analyst on the profiling team observed that Jewell's statement that he was hoping to get a position in the Atlanta Police Department after the games ended was highly inappropriate in the context of a lethal bombing and could indicate a motive for planting the explosives.

By the end of the day, Jewell had been transformed from a helpful witness to the FBI's principal suspect in the investigation, according to an FBI summary report prepared by its Office of Professional Integrity. In the late afternoon of 29 July, two FBI agents drove to Jewell's mother's apartment, where Jewell was staying—and where TV crews were already staked out. Jewell voluntarily agreed to drive down to the FBI offices in Atlanta to be interviewed.

The pace of the investigation—and Jewell's life—changed dramatically the next day, when the *Atlanta Journal-Constitution* stated in its 30 July edition that "the security guard who first alerted police to the pipe bomb that exploded in Centennial Olympic Park is the focus of the federal investigation into the incident."⁴⁰ The story noted that Jewell's profile fit the profile of a lone bomber and that Jewell had been approaching news organizations, trying to make himself into a celebrity. Jewell had in fact appeared on several programs, including CNN's *Talk Back Live*, NBC's *Today Show*, and *NBC News*, and had been cited in several newspapers, including the *Boston Globe*, the *Washington Post*, and *USA Today*. In these interviews, he discussed the sufficiency of training for security guards, the adequacy of the preparations for a possible bombing, whether authorities had responded properly to the event, and whether it was safe for people to return to Centennial Park.⁴¹ Jewell's attorney later claimed, however, that the media

relations coordinator for AT&T had “arranged for Mr. Jewell to participate in a limited number of media interviews” and that Jewell did so “to accommodate” his employer.⁴²

Subsequent press stories reported that Jewell possessed a knapsack similar to the one that contained the bomb, had been dismissed previously from two law enforcement positions, and had received bomb training at the Habersham County Sheriff’s Department. Questions were also raised in the press as to whether his voice matched that of the 911 caller.⁴³ Such press revelations put intense pressure on local, state, and federal investigators to solve the crime.

On 10 August, the *Atlanta Journal-Constitution* reported that Jewell’s defense lawyer claimed that it was physically impossible for Jewell to have made the 911 call given his known whereabouts at the time of the blast.⁴⁴ The telephoned bomb threat came about one minute after Jewell had alerted Tom Davis to the suspicious package. Investigators estimated that it would have taken about four minutes and forty-five seconds to walk from Centennial Park to the Days Inn where the phone call was placed, which meant that Jewell could not have placed the call.⁴⁵ More likely, Jewell was helping clear the park when the phone call was made. Some retorted, however, that the timing suggested Jewell had an accomplice in the crime.



Richard Jewell testifies about the Atlanta Olympics bombing before a House subcommittee on 30 July 1997.

As authorities built the case against Jewell, conflicting evidence began to surface suggesting that Jewell might not have been the perpetrator of the crime. On 20 August, the *Atlanta Journal-Constitution* reported that Jewell had passed a polygraph in which he denied any involvement in the bombing. A retired FBI polygraph expert conducted the examination.⁴⁶ A week later, Jewell’s mother attended a news conference called by her son’s attorneys and asked President Bill Clinton to intervene and exonerate Jewell. Attorney General Janet Reno refused to exonerate Jewell but did say, “I understand how she must feel.”⁴⁷ The authorities, however, pressed on with their investigation.

RECOMMENDED READINGS

Federal Bureau of Investigation, Counterterrorism Division, Counterterrorism Threat Assessment and Warning Unit, National Security Division. "Terrorism in the United States: 1996." 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>.

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. 300	Decision Support
Multiple Hypotheses Generator™	p. 173	Hypothesis Generation and Testing

THE ATLANTA OLYMPICS BOMBING

Structured Analytic Techniques in Action

Police investigators were under severe pressure to bring the investigation to closure quickly and to identify a prime suspect. Such dynamics make analysts and investigators vulnerable to groupthink; often they respond by adopting satisficing strategies that would please all key stakeholders. The best way to cope with such pressure is to employ structured techniques that require investigators and analysts to stop and think for a few minutes or hours before plunging in to resolve the case. This case study explores how three structured analytic techniques—the Key Assumption Check, Pros-Cons-Faults-and-Fixes, and the Multiple Hypotheses Generator™—can be employed to better frame the problem and avoid pursuing investigative blind alleys.

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. 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.

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.

Table 10.2 ▶ Key Assumptions Check Template			
Question: What assumptions are we making about Richard Jewell and the bombing in Centennial Park?			
Key Assumption	Supported	With Caveats	Unsupported
1.			
2.			
3.			
4.			

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.

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 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 question: 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.”

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

STEP 8: Consider whether key uncertainties should be converted into investigative leads, collection requirements, or research topics.

Analytic Value Added. What assumptions, if any, did law enforcement analysts and officials make as they began the investigation? Were they influenced by key assumptions of others, including the press and the experts they interviewed, who wanted to assist their work? Did the investigators fall into the trap of groupthink, or did they have sufficient cause to focus on Jewell as a suspect? What impact did key assumptions have on how effectively the FBI organized its investigation?

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.

STEP 1: Clearly define the proposed action or choice.

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.

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.

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.

STEP 6: Compare the Pros, including any Faults, against the Cons and Fixes (see Table 10.3).

Table 10.3 ▶ Pros-Cons-Faults-and-Fixes Template				
	Faults	Pros	Cons	Fixes
	Describe any Faults for Pro 1	Pro 1	Con 1	Describe any Fixes for Con 1
	Describe any Faults for Pro 2	Pro 2	Con 2	Describe any Fixes for Con 2
	Describe any Faults for Pro 3	Pro 3	Con 3	Describe any Fixes for Con 3

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?

Technique 3: 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.

Task 3. Use the Multiple Hypotheses Generator™ to create and assess alternative hypotheses for the bombing in Centennial Park. 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? (see Table 10.4).

Table 10.4 ▶ Multiple Hypotheses Generator™ Template				
Lead Hypothesis:				
Components	Lead Hypothesis	Alternative/Brainstormed		
Who?				
What?				
How?				
When?				
Where?				
Why?				

STEPS 2 AND 3: Identify plausible alternatives for each key component and strive to keep them mutually exclusive. Discard any “given” factors.

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.

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

STEP 8: Restate the permutations 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.

Analytic Value Added. Which hypotheses should be explored further? What motives should be considered, and why? Which hypotheses from the original list were set aside, and why?

NOTES

1. Federal Bureau of Investigation, Counterterrorism Division, Counterterrorism Threat Assessment and Warning Unit, National Security Division, “Terrorism in the United States: 1996,” 1996, http://www.fbi.gov/stats-services/publications/terror_96.pdf; Stephen Wilson, “Olympics Security Challenged,” *Washington Post*, July 27, 1996, <http://www.washingtonpost.com/wp-srv/national/longterm/bombing/stories/security.htm>.

2. BBC, “1996: Bomb Rocks Atlanta Olympics,” http://news.bbc.co.uk/onthisday/hi/dates/stories/july/27/newsid_3920000/3920865.stm.

3. Ibid.

4. FBI National Press Office, “Statement by Woody R. Enderson, Inspector in Charge of the Southeast Bomb Task Force” [press release], July 20, 1999.

5. 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; William Booth and Thomas Heath, “Bomb Tip May Have Set Up Police in Atlanta for ‘Ambush,’” July 30, 1996, *Washington Post*, <http://www.washingtonpost.com/wp-srv/national/longterm/bombing/stories/ambush.htm>.

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. Booth and Heath, “Bomb Tip May Have Set Up Police.”

9. Joan Kirchner, “How Olympic Bomb Was Found,” Associated Press, in *Washington Post*, July 27, 1996, <http://www.washingtonpost.com/wp-srv/national/longterm/bombing/stories/found.htm>.

10. Tom Beardon, “Security Matters” [transcript], PBS, July 29, 1996, http://www.pbs.org/newshour/bb/sports/july96/olympics_7-29.html.

11. Federal Bureau of Investigation, “Terrorism in the United States: 1996.”

12. Wilson, “Olympics Security Challenged.”

13. Ibid.

14. Lisa Beyer, “The Myths and Realities of Munich,” *Time*, December 4, 2005, <http://www.time.com/time/magazine/article/0,9171,1137646-1,00.html>.

15. Lopresti, “A Decade Later, Atlanta Olympic Bombing Overshadowed.”

16. Kirchner, “How Olympic Bomb Was Found.”

17. Booth and Heath, “Bomb Tip May Have Set Up Police.”

18. Ibid.

19. Ibid.

20. Ibid.
21. Beardon, "Security Matters."
22. Booth and Heath, "Bomb Tip May Have Set Up Police."
23. CNN, "Investigators Have Handful of Suspects," July 29, 1996, <http://edition.cnn.com/US/9607/29/bombing.clues/index.html>.
24. Kevin Sack, "No Arrests Imminent in Atlanta Bombing, F.B.I. Chief Says," *New York Times*, August 2, 1996, <http://www.nytimes.com/1996/08/02/us/no-arrests-imminent-in-atlanta-bombing-fbi-chief-says.html>.
25. Booth and Heath, "Bomb Tip May Have Set Up Police."
26. Dick Pettys, "Source: Atlanta Cops Waited," Associated Press, *Washington Post*, July 30, 1996, <http://www.washingtonpost.com/wp-srv/national/longterm/bombing/stories/10min.htm>.
27. Booth and Heath, "Bomb Tip May Have Set Up Police."
28. Ibid.
29. Ibid.
30. Ibid.
31. CNN, "Investigators Have 'Handful' of Suspects."
32. Booth and Heath, "Bomb Tip May Have Set Up Police."
33. FBI National Press Office, "Statement of FBI SAC Jack A. Daulton and Inspector Woody R. Enderson" [press release], November 18, 1997, <http://web.archive.org/web/20000303015458/www.fbi.gov/majcases/rudolph/presre11.htm>.
34. Booth and Heath, "Bomb Tip May Have Set Up Police."
35. Ron Ostrow, "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>.
36. Ibid.
37. Ibid.
38. Ibid.
39. Ibid.
40. Kathy Scruggs and Ron Martz, "FBI Suspects 'Hero' Guard May Have Planted Bomb," *Atlanta Journal-Constitution*, July 30, 1996, <http://www.journalism.org/print/1793>.
41. Ostrow, "Richard Jewell and the Olympic Bombing."
42. Clay Calvert and Robert D. Richards, "A Pyrrhic Press Victory: Why Holding Richard Jewell Is a Public Figure Is Wrong and Harms Journalism," *Loyola of Los Angeles Entertainment Law Review* 22, no. 2 (2002): 293–326, <http://elr.lls.edu/issues/v22-issue2/calvert.pdf>.
43. Ostrow, "Richard Jewell and the Olympic Bombing."
44. "Timing Indicates Jewell Did Not Make Bomb Threat," *Atlanta Journal-Constitution*, August 10, 1996, [http://nl.newsbank.com/nl-search/we/Archives?p_product=AT&p_theme=at&p_action=search&p_maxdocs=200&p_field_label-0=Author&p_field_label-1=title&p_bool_label-1=AND&s_dispstring=jewell%20911%20calls%20AND%20date\(all\)&p_field_advanced-0=&p_text_advanced-0=\(jewell%20911%20calls\)&p_perpage=10&p_sort=_rank_:D&xcal_ranksort=4&xcal_useweights=yes](http://nl.newsbank.com/nl-search/we/Archives?p_product=AT&p_theme=at&p_action=search&p_maxdocs=200&p_field_label-0=Author&p_field_label-1=title&p_bool_label-1=AND&s_dispstring=jewell%20911%20calls%20AND%20date(all)&p_field_advanced-0=&p_text_advanced-0=(jewell%20911%20calls)&p_perpage=10&p_sort=_rank_:D&xcal_ranksort=4&xcal_useweights=yes).
45. Ibid.
46. "Guard Questioned in Blast Passes Lie Detector Test," *Atlanta Journal-Constitution*, August 20, 1996, [http://nl.newsbank.com/nl-search/we/Archives?p_product=AT&p_theme=at&p_action=search&p_maxdocs=200&p_field_label-0=Author&p_field_label-1=title&p_bool_label-1=AND&s_dispstring=jewell%20polygraph%20AND%20date\(08/01/1996%20to%2008/22/1996\)&p_field_date-0=YMD_date&p_params_date-0=date:B,E&p_text_date-0=08/01/1996%20to%2008/22/1996\)&p_field_advanced-0=&p_text_advanced-0=\(jewell%20polygraph\)&p_perpage=10&p_sort=_rank_:D&xcal_ranksort=4&xcal_useweights=yes](http://nl.newsbank.com/nl-search/we/Archives?p_product=AT&p_theme=at&p_action=search&p_maxdocs=200&p_field_label-0=Author&p_field_label-1=title&p_bool_label-1=AND&s_dispstring=jewell%20polygraph%20AND%20date(08/01/1996%20to%2008/22/1996)&p_field_date-0=YMD_date&p_params_date-0=date:B,E&p_text_date-0=08/01/1996%20to%2008/22/1996)&p_field_advanced-0=&p_text_advanced-0=(jewell%20polygraph)&p_perpage=10&p_sort=_rank_:D&xcal_ranksort=4&xcal_useweights=yes).
47. Tribune News Service, "Sympathy, No Apology, for Jewell's Mom," *Chicago Tribune*, August 30, 1996, http://articles.chicagotribune.com/1996-08-30/news/9608300140_1_security-guard-richard-jewell-centennial-olympic-park-bombing-barbara-jewell.

11 The DC Sniper

Key Questions

- ▶ What hard evidence did investigators collect?
- ▶ What was the profile of the prime suspect?
- ▶ Did investigators consider alternative suspects, and why?
- ▶ What key decision points did investigators face?
- ▶ Should investigators have released more or less information to the public about the shootings?

CASE NARRATIVE

On Wednesday, 2 October 2002, three weeks to the day after the first anniversary of the 11 September 2001 terrorist attacks, the American psyche was still focused on the seemingly ever-present threat of a terrorist attack on the homeland. However, it was business as usual in the suburbs of the nation's capital until a strange event occurred at Michael's Arts and Crafts store in Montgomery County, Maryland. At 1702, someone shot a single bullet into the store, located at 13850 Georgia Avenue in the Aspen Hill neighborhood.¹ No one was injured. The bullet entered the store and struck a checkout aisle register number, just a few feet above the head of a cashier. The investigators who responded to the incident found no evidence, no motive, and no suspect. The only witness report, a tentative description of two African American men in a Thunderbird-like blue car, was dismissed as being in an improbable location relative to the shooting.² Investigators did not know at the time that events were about to evolve from bizarre to nightmarish.

The Killings Begin

Approximately an hour after the Michael's shooting at 1802, James Martin, a fifty-five-year-old white father of an eighteen-year-old son, was shot and killed as he walked from his car to a Shoppers Food Warehouse located at 2201 Randolph Road, Wheaton, a neighborhood of Montgomery County, Maryland.³ The shopping center, only a few miles from Aspen Hill, was across the street from a police station.

At first, investigators handled the case as a normal homicide. The only solid information that witnesses—including the responding officer, who had been in his parked vehicle across the street—provided was hearing a loud boom. No one saw the shooter. One witness report identified a

white sedan, possibly a Toyota, but that too was discounted as improbable because of its reported position relative to the victim.⁴ In addition, there was no immediately apparent motive; the victim was not robbed, and his work identification badge was still on his chest.

An examination of the wound in Martin's body was indicative of a high-powered rifle. Investigators initially suspected a .223-caliber or similar-sized round.⁵ They hoped the autopsy would confirm this suspicion and provide additional information. In addition to no apparent motive, there was no suspect or suspect vehicle and little to no real evidence. It did not take long for investigators to consider the possibility that the two cases were somehow linked, which caused a chilling thought: "Who is out there just shooting someone for no apparent reason right across from the police station in broad daylight at rush hour?"⁶

At 0741 the next day, James L. "Sonny" Buchanan, a thirty-nine-year-old white male, suffered a major chest wound and died while mowing the grass at Colonial Dodge in the Fitzgerald Auto Mall, located at 11411 Rockville Pike in Kensington, Maryland.⁷ It was initially reported that some kind of mower malfunction had killed him. However, it was soon clear that he had been shot. As with the other two shootings, there was no witness, no evidence, no suspect or suspect vehicle, and still no motive. And while it too was incredibly strange, nothing immediately linked this shooting to the other two shootings the day before.

As the Montgomery County Police Department (MCPD) began to handle the Buchanan homicide, Premkumar A. Walekar, a fifty-four-year-old Indian-born male, lay dying at a Mobil gas station located at Aspen Hill Road and Connecticut Avenue in Aspen Hill.⁸ He had been putting gas in his taxi when he was fatally shot at 0802 in the same manner as Buchanan and Martin. In this case, an officer was sitting in a patrol car in heavy traffic at an intersection about fifty yards away.⁹

As with the other shootings, Walekar was not robbed, and there were no witnesses or evidence. Investigators worked to account for the sudden increase in homicides. Montgomery County averages only about twenty homicides a year.¹⁰ Now there had been three in a matter of hours. The investigators considered and immediately dismissed the shootings as either the result of a domestic crime or robbery, the most common explanations for a homicide.

About forty minutes later, at 0837, Sarah Ramos, a thirty-four-year-old Hispanic mother of a seven-year-old son, was sitting at a bus stop in front of a post office located at 3701 Rossmoor Boulevard, Silver Spring, Maryland.¹¹ Witnesses later reported hearing a popping sound. A Spanish-speaking witness reported seeing a white box truck with black lettering drive away from the area after Ramos was shot.¹² The police later that day revealed the white box truck lead in a press conference. The media reported it extensively, and investigators considered it a significant lead in the case.

At 0958, Lori Lewis-Rivera, a twenty-three-year-old white woman, was fatally shot while purchasing gas at a Shell station located at Knowles and Connecticut Avenue in Kensington, Maryland, only about a mile from the parking lot of the Mobil station where the investigation of Ramos's death was still ongoing.¹³ This was the sixth shooting in seventeen hours, the fifth death overall, and the fourth death in a little over two hours.

At this point, the police set up a command post at a church near the Mobil gas station. Because the shootings all appeared to be centered on the Aspen Hill area, law enforcement devoted all resources to that area. Police began to consider additional reasons for the killing spree, such as a racial crime, a hate crime, or a terrorist act. They ultimately discounted these

theories, particularly terrorism, and instead focused on finding a link among the victims in the hope of gaining insight into the murderer. The investigators thought that some common thread must connect the victims.¹⁴

On Thursday afternoon, the police asked citizens to call in suspicious activity to 911, especially information about white vans. They also moved the command post back to the station in Rockville, Maryland. Forensics began working on the bullet fragments from the victims, and the coroner conducted autopsies on the victims.

At 2120 on Thursday, Pascal Charlot, a seventy-two-year-old black male carpenter originally from Haiti, was shot and killed as he was about to cross a street at the intersection of Georgia Avenue and Kalmia Road.¹⁵ This shooting was like all the rest, with one major exception: it occurred in the District of Columbia, not in Montgomery County. Still, the shooting was just over the county line. The police thought they might have captured the shooter when a car ran a red light at the same time as the shooting, but this turned out to be a false lead.¹⁶ One witness also reported that a burgundy Caprice left the area, but the vehicle was later found abandoned and burned¹⁷ and was discounted as a suspect vehicle.¹⁸

Also different in the Charlot shooting was that for the first time, the police were able to use dogs to trace the gunpowder residue of the shot. The police now knew exactly the type of gun used, and although this did not help identify the shooter, the police could identify and confirm the type of weapon used: a high-powered rifle.

Investigators Join Forces

On Friday, investigators from the ever-growing investigation team met to discuss what, if anything, they had determined. MCPD; the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the Federal Bureau of Investigation; and the Washington Metropolitan Police Department (WMPD) joined in the investigation, although an official Joint Command was not yet formed. The investigators knew the same caliber shot was used in each shooting, most likely a .223 round. They also knew the shots were fired from 100–150 yards away from each victim. For the most part, they were able to determine the general area the shots were taken from by studying the trajectory path of each shot.¹⁹ But that was it: no motive, no suspects, and no known links between victims. There was nothing solid to act upon, although tips came in through 911. Investigators still could not confirm a connection between the shooting at Michael's and other shootings because there were no shell fragments or victims from the Michael's shooting.

At 1430 on Friday, about the time the investigators were meeting, Caroline Seawell, a forty-three-year-old white woman, was in the parking lot of the Spotsylvania Mall in front of a Michael's located at 3000 Plank Road, Fredericksburg, Virginia, when she was shot.²⁰ This time a witness reported having seen a dark-colored car with tinted windows and New Jersey tags in the area, and another witness reported seeing a black teenager inside it, but it is unclear whether the investigators in Maryland knew about the report at the time or, if they did, whether they discounted it.²¹ The shooting was much like the others, but Seawell survived. Investigators thought the shooter was moving south and began warning police agencies in that direction.

Saturday and Sunday came and went without incident. Police on Saturday announced that ballistics tests on the bullet fragments indicated that four of the victims had been shot by the same weapon and that they were pursuing a serial killer. MCPD reconfirmed that it was looking for a white box truck, possibly with black lettering on the side.²²

On Monday, 7 October, at 0809, Iran Brown, a thirteen-year-old male, was shot as he was walking into Tasker Middle School located at 490 Collington Road, Bowie, Maryland, in Prince George's County.²³ Prior to this, the commonly held belief was that the schools were safe, and officers had even been stationed at some schools to ensure the students' safety. Brown barely survived the attack, but as with previous shootings, there were no witnesses and no suspect. The police extensively searched the area and even used police academy recruits to assist. Their efforts resulted in finding a shell casing and, more important, a tarot card, the Death card (see Figure 11.1), with the words "For you Mr. Police. Code: 'Call me God.' Do not release to the press."²⁴ It was regarded by all to be a message from the shooter. The police decided to honor the request of the sniper, but the message was leaked to the press. However, the press incorrectly reported the phrase that appeared on the card. One variation commonly reported was "I am God."²⁵

After the Brown shooting but before the police knew of the tarot card, the chief of MCPD submitted a formal request for assistance to the federal government. The US attorney general responded immediately and personally.²⁶ Within a short time the Secret Service, US marshals, and even the Department of Defense made new resources available. In addition, FBI resources dramatically increased, and the Bureau formalized its contribution to the investigation. Police created a Joint Operations Center (JOC) to coordinate the investigation, and they officially named the task force SNIPEMUR.

Figure 11.1 ▶ Tarot Card Found at Site of Iran Brown Shooting



Source: <http://www.fbi.gov/page2/oct07/snipers102407.html>.

Figure 11.2 ▶ FBI Profile of DC Sniper



- Single Shooter
- Adult White Male
- Washington Area
- Military Exposure
- Non-Confrontational
- Angry, Self-Centered
- Competent w/Firearms
- Little to No Criminal History
- Uninvolved Romantically

In an attempt to identify the shooter, investigators tried to identify all owners of rifles capable of firing a .223 round in Virginia and Maryland. They cross-referenced their findings to owners of white vans.²⁷ Tips on such owners even came through the tip line. The leads, however, never resulted in a link to the shooter.

A Profile Emerges

The FBI stepped in to create a profile of the killer for the investigation (see Figure 11.2). Although this profile was not released to the public, a similar profile was extensively discussed by the media. The FBI profile described the attacks as

probably the work of a single shooter.... The sniper was likely angry, self-centered, and fascinated with weapons and violence. Probably the sniper had recently suffered a domestic or job related setback. He would stay in the Washington area, keep the same method of operation, and scout his shooting locations. The sniper was almost certainly male, was probably not a juvenile, and was not likely to display any sign of mental illness.²⁸

The profile described an individual who frequented gun shows, was interested in books and movies about the military, and took pride in his prowess with firearms. He would most likely take calculated risks, not be confrontational, and not be involved in a long-term relationship. He would come and go as he pleased. He would be hypersensitive and suspicious and pay close attention to media coverage.²⁹

The profilers pointed out that although race could not be identified, “historically similar cases have been perpetrated by white males.”³⁰ The FBI profilers could not find a link or common trait among the victims. They also commented that the shooter would most likely be “competent with firearms...not likely have a lengthy criminal history...an angry person...of average or above average intelligence.”³¹

The investigators had many leads consistent with the FBI profile but ruled them all out. This

pattern continued for days. Police tracked dozens of leads and suspects who fit the profile, but all ultimately resulted in dead ends. The police, however, never released any suspect information to the press.

On Wednesday, 9 October, at 2010, Dean Harold Meyers, a fifty-three-year-old disabled Vietnam veteran, was pumping gas at a Sunoco gas station located at 7203 Sudley Road near Manassas, Virginia, off of I-66, when he was fatally shot.³² This shooting followed the same pattern as all the others. Witnesses heard a loud noise as Meyers went down. A white van was reported fleeing the area, but it was identified and found to be unrelated to the incident. Investigators found a map of Baltimore and Baltimore County across the street, but they neither processed it nor gave it to the task force. Instead, investigators sent it to an evidence locker.³³

By Thursday morning, the new JOC was fully operational in a rented building across from the MCPD station. A new tip line was created just to handle calls regarding the sniper. The tips received ranged from helpful to bizarre to useless. Investigators tried to track down every lead from the more reliable tips.

The media continued to spiral out of control. As the death toll climbed, media from around the world covered the incident ever more fervently. Criticisms of the police surfaced, and some demanded to have the tarot card made fully public. The police did not honor the request.

On Friday, 11 October, at 0930, Kenneth H. Bridges, a fifty-three-year-old black father of six, was pumping gas at an Exxon station located at US-1 and Market Street, Fredericksburg, Virginia, when he was shot.³⁴ Much as with the Buchanan murder, a state trooper was about fifty yards away.³⁵ A witness reported seeing a white Astro van with ladder racks flee the area.³⁶ There was no evidence, no message, and no suspect.

The police had already created a dragnet plan whereby they would shut down the roadway system as they attempted to find the fleeing white van. The Bridges shooting was the first time the plan went live.³⁷ In response to the shooting, police across the area pulled over hundreds of white vans.³⁸ None were connected to the shooting. Traffic, however, ground to a halt.

On the same day, SNIPEMUR had another meeting. The status had not changed much; the investigators had very little evidence. They knew the same weapon was being used for each killing, but some worried that the killer might switch weapons. Some in attendance even began to raise concerns about the validity of the white van. One of the commanders of SNIPEMUR tried to encourage the investigators to “think three murders ahead.”³⁹ Despite any initial internal dissent about the white van, investigators released a composite graphic of the vehicle based on reports from the 3 October shootings to the press.⁴⁰

After two days without incident, at 2115 on Columbus Day, Monday, 14 October, Linda Franklin, a forty-seven-year-old FBI analyst and mother of two, was shot and killed at a Home Depot located at 6210 Seven Corners Center, Falls Church, Virginia.⁴¹ The ensuing dragnet shut down I-495, the George Washington Parkway, the American Legion Bridge, and the Woodrow Wilson Bridge. The police also had a witness with a criminal record who said he saw the shooting. The witness said that “it was a cream-colored Chevy Astro van with a silver ladder rack and a dead right taillight. The gunman had olive skin and a mustache and wore a denim jacket with a rifle similar to an AK-47.”⁴² With this information, the task force and dragnet focused even more on a white van. Once again, SNIPEMUR attempted to identify owners of white vans, this time Chevy Astros, who also owned .223 rifles.⁴³ As with the previous dragnet and attempt to match van and weapon to a suspect, nothing came of it.

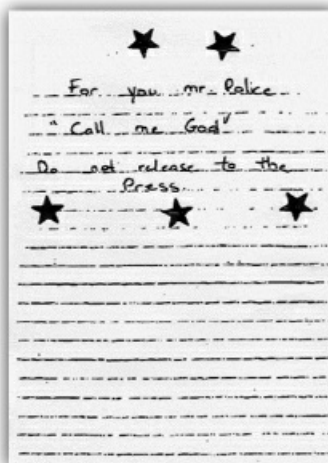
On 16 October, it became clear the witness was lying. He had been inside the store when the shot was fired.⁴⁴ By 18 October, the police had arrested the witness “for providing false information to police.”⁴⁵

Leads continued to be tracked down but ultimately dismissed. There were more leads than the now-massive task force could handle, but the investigators did their best. A few days went by without incident, and some began to wonder whether the shooter had stopped. But on Saturday, 19 October, at 2000, Jeff Hopper, a thirty-seven-year-old white male, was leaving the Ponderosa Steak House located at 809 England Street, Ashland, Virginia, with his wife when he was shot in the same style as all the other victims. Like Seawell and Brown, he survived.⁴⁶ Still, no witness saw anything.

A Break in the Case

Just as in the Charlot shooting, investigators used dogs at the scene, and they found a note (Figure 11.3) with language similar to that used on the tarot card.⁴⁷ The media had misreported the tarot card language, so the use of similar language in the new note suggested to investigators that the message was authentic. The message contained references to past attempts to contact the police as well as a demand for \$10 million to be deposited to a Platinum Visa credit card account.⁴⁸ The note contained threats of future killings if the demand was not met. According to the note, the police would receive a phone call with further instructions Sunday at 0600 at the Ponderosa. The problem was that by the time the letter had been processed and read, it was already 0800 on Sunday. There were other complications as well: the note had the wrong number for the Ponderosa, and the Ponderosa was not open at 0600 on Sundays.⁴⁹ The note also said the money had to be deposited by Monday at 0900.

Figure 11.3 ▶ First Page of Letter Found at Ponderosa Steak House



Source: E-mail from Media Service Division, Montgomery County Department of Police, to Pherson Associates, 19 August 2009.

This note posed a number of issues for SNIPEMUR. There was debate about whether or not to proceed and deposit money into the account in the hopes of catching the shooter during a withdrawal. Some were concerned about the feasibility of catching the shooter this way and whether it was worth the risk. The card number provided had been stolen and therefore deactivated; although it could be reactivated, it did not appear that the use of the card could be reported fast enough in real time to ensure a capture.⁵⁰

There was also debate about how to continue the dialogue with the shooter because the deadline to speak on the phone had passed. This issue caused significant discord in SNIPEMUR. On the one hand, the trained negotiators wanted the police to take a very hard line with the shooter. They wanted to use strong language that would “call out” the sniper.⁵¹ On the other hand, the profilers wanted a much more reserved approach. They wanted the police to engage the shooter in a nonthreatening manner in order to draw out information that could help identify the sniper.

The task force managed to agree to put out a message via the media asking for the shooter to reattempt contact. On Sunday, the police issued the statement saying that they had been unable to comply but wanted to talk. Someone did call the task force the next day. Officers had been staged around the area of the Ponderosa in the belief the caller might still be around. When the call came in, police attempted to capture the caller, but it was too late—the caller was gone. Instead, police mistakenly picked up two undocumented immigrants.

The caller used the same phrases as were in the letter. Once again, threats were made if the demand was not met. But the caller ended the call quickly, and no further dialogue was possible. The person spoke with an accent most commonly described as Hispanic. The police once again released a message via the media asking the shooter to call back so they could better understand the demand.

On Tuesday, 22 October, at 0555, Conrad Johnson, a thirty-five-year-old father of two, stood in the door of a public bus at Grand Pre Road and Connecticut Avenue in Aspen Hill, Maryland, when he was shot and killed.⁵² Yet another death, and still no one saw the shooter. Investigators found another note. It reiterated the other messages and said, “Your incompetence has cost you another life.”⁵³ Johnson’s would be the last life lost. Map 11.1 details the locations of the sniper shootings.

The End of the Terror

Two days later, it all came to an end. At last, after three weeks of living a nightmare, the people in Maryland, Virginia, and the District of Columbia no longer had to fear being shot by a ghostlike gunman. All of the frustration and sleepless nights for the task force were replaced with a sense of accomplishment at ending the madness of the DC Sniper.

RECOMMENDED READING

Moose, Charles, and Charles Fleming. *Three Weeks in October: The Manhunt for the Serial Sniper*. New York: Signet, 2003.

Map 11.1 ► Locations of the Sniper Shootings in the Washington, D.C., Region

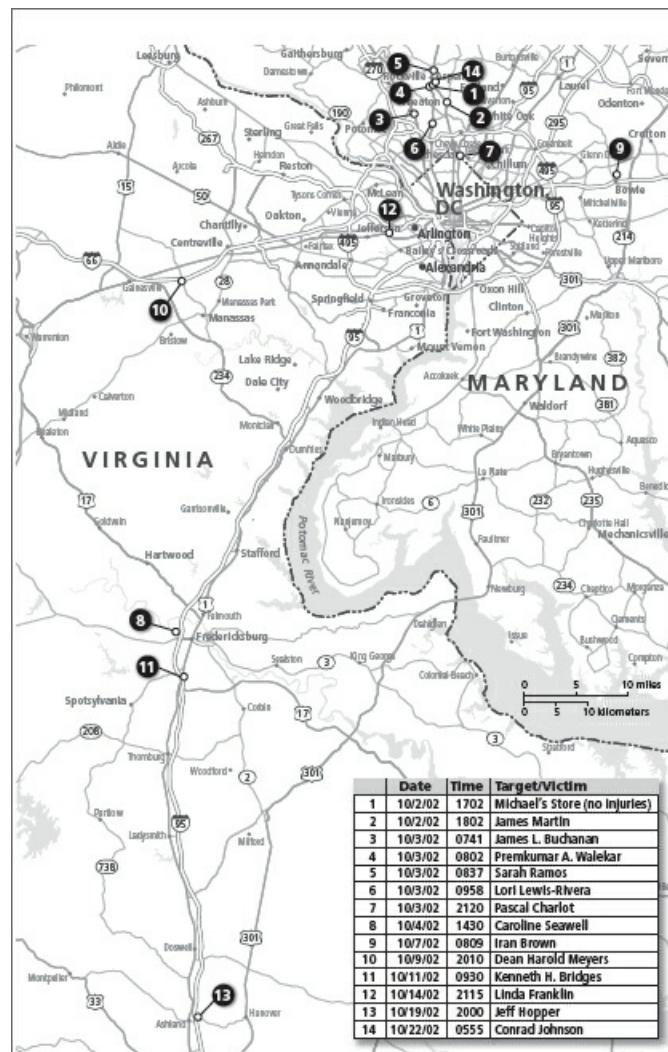


Table 11.1 ► Case Snapshot: The DC Sniper

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

THE DC SNIPER

Structured Analytic Techniques in Action

In a crisis situation, using structured analytic techniques can help avoid a rush to judgment and ensure that no possibility has been prematurely discarded. Investigators in the case were challenged by the lack of hard evidence about the perpetrator, including the mode of transportation and motive for the crimes, the fast pace of the shooting spree, and a deluge of eyewitness information that overwhelmed the task force. The Key Assumptions Check in this case helps to explicate and challenge implicit assumptions about the sniper, while the Multiple Hypotheses Generator™ and Classic Quadrant Crunching™ exercises systematically develop and assess a range of possible explanations.

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.
- 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.

Table 11.2 ▶ Key Assumptions Check Template

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

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.

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"

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

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?

Technique 2: Multiple Hypotheses GeneratorTM

The Multiple Hypotheses GeneratorTM is a useful tool for broadening the spectrum of plausible hypotheses. It is particularly useful when there is a reigning lead hypotheses—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 GeneratorTM (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.

STEPS 2 AND 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 11.3 ▶ Multiple Hypotheses Generator™ Template			
Lead Hypothesis: A white male is driving a white van and killing to extort money.			
Components	Lead Hypothesis	Alternatives Brainstormed	
Who?			
What?			
Why?			

STEPS 4, 5, AND 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.

STEP 7: Re-sort the remaining hypotheses from most to least credible.

STEP 8: Restate the permutations 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.

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?

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.

STEPS 1 AND 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.

Table 11.4 ▶ Classic Quadrant Crunching™ Matrix Template

Key Assumptions	Contrary Assumptions	Contrary Dimensions

Step 3. Identify contrary assumptions and two contrary dimensions in a template like that shown in Table 11.4.

Step 4. Array combinations of these contrary assumptions in a set of 2×2 matrices.

Step 5. Generate scenarios for each quadrant.

Step 6. Select those scenarios (cells) deserving the most attention.

Step 7. Develop indicators for the selected scenarios.

Analytic Value Added. Which alternative scenarios should investigators have pursued, and why?

NOTES

1. "2002 Area Sniper Shootings," *Washington Post*, August 4, 2009, <http://www.washingtonpost.com/wp-srv/metro/daily/oct02/snipershootings.htm>.
2. Sari Horwitz and Michael E. Ruane, *Sniper: Inside the Hunt for the Killers Who Terrorized the Nation* (New York: Random House, 2003), 15–16.
3. "Profiles of Those Killed," Fox News Online, October 23, 2002, <http://www.foxnews.com/story/0,2933,65519,00.html>; "2002 Area Sniper Shootings."
4. Horwitz and Ruane, *Sniper*, 11.
5. Ibid.; Charles Moose and Charles Fleming, *Three Weeks in October: The Manhunt for the Serial Sniper* (New York: Signet, 2003), 6.
6. Horwitz and Ruane, *Sniper*, 14.
7. "Profiles of Those Killed."; "2002 Area Sniper Shootings."
8. "Profiles of Those Killed."
9. "The Hunt for a Sniper: Death by the Highway; Fatal Shooting of Driver at Gasoline Station Intensifies Hunt for Suburban Sniper," *New York Times*, October 12, 2002, <http://www.nytimes.com/2002/10/12/us/hunt-for-sniper-death-highway-fatal-shooting-driver-gasoline-station-intensifies.html>.
10. "Quarterly Crime Report Year End 2002," Montgomery County Department of Police, April 29, 2003, http://www.montgomerycountymd.gov/content/Pol/crimestats/pdfs/2002_YearEnd.pdf.
11. "Profiles of Those Killed."; "2002 Area Sniper Shootings."
12. Ibid.
13. Ibid.
14. Moose and Fleming, *Three Weeks in October*, 32.
15. "2002 Area Sniper Shootings"; "Profiles of Those Killed."
16. Moose and Fleming, *Three Weeks in October*, 39.
17. A conflict exists between Chief Moose's account, which says the car was found abandoned and burned out, and the book by Horwitz and Ruane, which says the car that fled the scene was a red Toyota and that the driver was identified and discounted. Neither book mentions why the car was discounted, and we have used the more detailed version by Chief Moose here.

18. Moose and Fleming, *Three Weeks in October*, 32.
19. Ibid., 72–74.
20. Ibid., 74.
21. The description of the dark-colored car with New Jersey tags appears in the book by Horwitz and Ruane, but Chief Moose, in his book, reported no eyewitnesses. The Horwitz and Ruane book does not make it clear whether the police were informed of the vehicle despite two witnesses claiming they saw it. Horwitz and Ruane, *Sniper*, 104.
22. Moose and Fleming, *Three Weeks in October*, 86.
23. Horwitz and Ruane, *Sniper*, 111.
24. A conflict regarding the phrase on the tarot card exists between the account in the book by Horwitz and Ruane and the account by Chief Moose (131). The version by Horwitz and Ruane has been used here because it matches the wording on the image of the tarot card from the FBI. Horwitz and Ruane, *Sniper*, 119.
25. “Man Killed at Suburban D.C. Gas Station,” CNN, October 10, 2002, <http://edition.cnn.com/2002/US/South/10/09/shootings.maryland/index.html>.
26. Moose and Fleming, *Three Weeks in October*, 141.
27. Ibid., 144–45.
28. Horwitz and Ruane, *Sniper*, 102.
29. Ibid.
30. Moose and Fleming, *Three Weeks in October*, 150.
31. Ibid.
32. “Profiles of Those Killed”; “2002 Area Sniper Shootings.”
33. Horwitz and Ruane, *Sniper*, 130–31.
34. “Profiles of Those Killed”; “2002 Area Sniper Shootings.”
35. Horwitz and Ruane, *Sniper*, 140.
36. “2002 Area Sniper Shootings”; Horwitz and Ruane, *Sniper*, 141.
37. The book by Horwitz and Ruane and the account of Chief Moose offer conflicting information about when the first dragnet occurred. Chief Moose specifically says a dragnet was first used in the Franklin murder, but Horwitz and Ruane refer to a Virginia dragnet that occurred after the Bridges murder. Moose may be referring to the first dragnet by the task force itself instead of the first instance of a dragnet.
38. Horwitz and Ruane, *Sniper*, 141.
39. Ibid., 145.
40. Ibid.
41. “Profiles of Those Killed”; “2002 Area Sniper Shootings.”
42. Horwitz and Ruane, *Sniper*, 153.
43. Ibid., 156.
44. Ibid., 162.
45. “Timeline: Tracking the Sniper’s Trail,” Fox News Online, October 2, 2002, <http://www.foxnews.com/story/0,2933,66630,00.html>.
46. “2002 Area Sniper Shootings”; Horwitz and Ruane, *Sniper*, 167.
47. Dogs had been used at all the scenes since the Charlot killing.
48. Moose and Fleming, *Three Weeks in October*, 246.
49. Ibid.
50. Ibid., 253.
51. Ibid., 255.
52. “Profiles of Those Killed”; “2002 Area Sniper Shootings.”
53. Horwitz and Ruane, *Sniper*, 188.

12 Colombia's FARC Attacks the US Homeland

Key Questions

- ▶ If Colombia's leading narco-insurgent group, the Revolutionary Armed Forces of Colombia (known by its Spanish acronym, the FARC), were planning to attack the US homeland, how would it go about it?
- ▶ What are the major factors that would influence the type of attack the FARC would launch? Who and what would be the most likely targets?
- ▶ What capabilities and resources could the FARC draw on internally to launch an attack against the United States?
- ▶ Would the FARC look to other groups for assistance in launching an attack?
- ▶ What events or activities would best signal that a FARC attack on the US homeland may be imminent?

CASE NARRATIVE

The Revolutionary Armed Forces of Colombia—known by the Spanish acronym FARC—is Latin America's largest, oldest, and currently most capable insurgent organization. Its history of kidnappings, assassinations, and indiscriminate acts of violence makes the FARC one of the most despised groups in Colombia and has landed it on the US State Department's list of foreign terrorist organizations.¹ In recent years, the FARC has cultivated relationships with foreign states, such as Venezuela and Ecuador, and terrorist groups, such as the Spanish Basque separatist group ETA and the Irish Republican Army, reportedly to gain access to military materiel and terrorist expertise. Since 2003, the Colombian government—with help from the US military—has cracked down on the FARC and its main source of income: the drug trade. Although this has led to operational successes, including the deaths of many FARC leaders, it has also raised the specter of increased violence against not only the Colombian government but also against the United States, as the FARC seeks to regroup and assert its revolutionary credentials.

Revolutionary Roots

The FARC was formally established in 1965 after Colombia's two major political parties ended more than a decade of political violence, a period known as *La Violencia*, which resulted in more than two hundred thousand deaths. Under this agreement, known as the National Front, the two

leading political parties agreed to share power, end the violence, and return the country to civilian rule.

The period from the late 1960s to the mid-1970s was the height of armed rebellion throughout Latin America. Funded in part by Cuba, leftist revolutionary groups operated throughout the continent. Since then, nearly all of the groups have been eliminated, legitimized, or disbanded—but not the FARC. Several factors account for the FARC's ability to survive when nearly all other armed communist insurgencies in Latin America have disappeared. Much of Colombia's territory is beyond the central government's control. Large parts of the Amazon region have provided safe haven to the FARC and other outlaw groups for decades. The FARC also has developed significant military capability and experience during forty years of armed struggle. But the most important factor contributing to the FARC's longevity has been a sustainable business model based on kidnapping for ransom, extortion, and, increasingly, the drug trade.

According to the Colombian government, the FARC had about sixteen thousand insurgents in 2001. The head of the United States Southern Command (USSOUTHCOM) testified in March 2008 that the FARC had been reduced to about nine thousand fighters. FARC forces are well equipped, and the group is known to use highly sophisticated technology. Its forces are mostly self-trained and self-supplied, although the FARC has recently received some external assistance.

The FARC is made up of about seventy-seven distinct military units, called Fronts, organized by geographic location. These in turn are grouped into seven "blocs." The FARC is led by a seven-member Secretariat and a twenty-seven-member Central General Staff, or *Estado Mayor*. The FARC is most active in the southern and eastern portions of the country, which are mostly jungle.² It also has an International Commission with representatives in Latin America, Europe, Canada, and the United States.³ The FARC maintains a series of websites to post its messages and attract followers within Colombia and overseas.



FARC rebels stand in formation during a practice ceremony.

In 1999, Colombian President Andres Pastrana tried to engage the FARC in peace negotiations. As part of this initiative, he gave it control over a forty-two-thousand-square-mile swath of jungle, which was called the *despeje*, or the "demilitarized zone." After three years of unsuccessful negotiations and in the wake of a series of high-profile terrorist attacks, Pastrana ended peace talks and ordered his troops to retake the *despeje*. When President Alvaro Uribe

came to power in 2002, he ordered a major military campaign against the FARC and its sister insurgency, the National Liberation Army (ELN). In 2007, several members of the FARC leadership were killed; in the following year, the FARC Secretariat's chief spokesperson, Raul Reyes, was killed during a Colombian incursion into Ecuador. The FARC suffered another major setback in July 2008 when Eastern Front commander Gerardo Aguilar Ramirez, also known as "Cesar," was captured as part of an operation to rescue three American hostages who had been held in captivity by the FARC since their plane crashed in February 2003.

The FARC's Terrorist Acts

The FARC is responsible for most of the ransom kidnappings in Colombia. It targets wealthy landowners, politicians, foreign tourists, and prominent Colombian and foreign officials. Notable FARC operations include the following:

- ▶ The March 1999 murder of three US missionaries working in Colombia
- ▶ The October 2001 kidnapping and murder of a former minister of culture
- ▶ The February 2002 kidnapping of presidential candidate Ingrid Betancourt, who was traveling in guerrilla territory
- ▶ The November 2005 kidnapping of sixty people, holding them hostage until the government agreed to release hundreds of FARC insurgents and sympathizers serving prison sentences⁴



Former Colombian presidential candidate Ingrid Betancourt is seen during her captivity in this image taken from television 31 August 2003.

The FARC is renowned for its reliance on assassinations and its use of mortarlike devices, called *rompas*, which the rebels fashion from empty natural gas canisters. In part because of its history of kidnappings, assassinations, and indiscriminate violent acts, the FARC is one of the most despised groups in Colombia. Opinion polls show that just 1 percent of Colombians hold a favorable view of the FARC.⁵

The FARC Builds Its Foreign Connections

When President Uribe launched his crackdown on the FARC and the ELN in 2003, both groups sought refuge across the border in Venezuela and Ecuador. The border areas have traditionally been hard to govern and thus are ideal places for arms smugglers and drug traffickers to operate. When Raul Reyes was killed in 2008, the Colombian government said it had found documents on a rebel's laptop that indicated that Venezuela and Ecuador were providing material support to the FARC.

In August 2009, the *New York Times* reported that evidence taken from an insurgent's laptop documented Venezuelan aid to the FARC. The messages describe FARC plans to purchase surface-to-air missiles, sniper rifles, and radios in Venezuela in 2008. The messages appear to corroborate the assertion that Venezuela helped the FARC acquire Swedish-made rocket launchers. The rocket launchers were purchased by the Venezuelan Army in the late 1980s but were captured in Colombia in combat operations against the FARC in 2008.⁶ In 2009, Venezuelan President Hugo Chávez denied providing such assistance and expressed concern over US plans to increase its military presence on Colombian military bases, claiming it would lead to the destabilization of the region.⁷

The FARC's ties to Venezuela and Spain's Basque separatist group ETA became a major issue in March 2010, when a Spanish judge charged thirteen members of the ETA and the FARC with planning to assassinate visiting senior Colombian officials, including President Uribe. The judge said a FARC member had carried out surveillance on the Colombian Embassy in Madrid and the routes taken by former Colombian president Pastrana, who lives in Spain. The FARC then asked the ETA to follow Pastrana, as well as the former ambassador to Spain Noemi Sanin, current Vice President Francisco Santos, and the former mayor of Bogotá Antanas Mockus, "with the aim of assassinating one of them when they were in Spain." Uribe was added later to that list. Six ETA members and seven FARC members were charged in the plot.⁸

Members of the Irish Republican Army (IRA) have also been accused of supporting the FARC. In April 2002, the US House Committee on International Relations issued a summary of a nine-month investigation that stated that links between the IRA and the Colombian guerrillas went back to 1998. The study noted that three IRA members were arrested in Colombia in August 2001 and accused of teaching bomb-making methods to FARC insurgents. According to the report, the training helped the rebels become proficient in urban terror techniques used by the IRA in Northern Ireland; two of the Irish were the IRA's leading explosives and mortar experts.⁹

The FARC's Role in the Drug Trade

Experts estimate that the FARC takes in roughly \$500 million annually from the illegal drug trade.¹⁰ The FARC also profits from kidnappings, extortion schemes, and an unofficial "tax" it levies in the countryside for protection and social services.

About half of the FARC's operational units are involved in some aspects of the drug trade, with most of this activity relating to managing local drug production.¹¹ (Map 12.1 shows the presence of the FARC across Colombia along with areas of coca cultivation.) The nature of the FARC's drug involvement varies from region to region, and the group's control of population and territory in rural areas "has allowed it to dictate terms for coca growth, harvest, and processing."¹²

Map 12.1 ▶ FARC Presence in Colombia and Coca Cultivation Areas



A press release issued by the US Department of Justice (DoJ) when Ramirez was extradited to the United States in July 2009 asserted that “the FARC is responsible for the production of more than half the world’s supply of cocaine and nearly two-thirds of the cocaine imported into the United States.” The press announcement stated that by the late 1990s, the FARC became the exclusive buyer of raw cocaine paste used to make cocaine in all areas of FARC operations.¹³ A 2009 report by the US Government Accountability Office says the FARC accounts for 60 percent of the total cocaine exported from Colombia to the United States.¹⁴

The DoJ press release also states that in the late 1990s, the FARC leadership met and voted unanimously in favor of expanding coca production, expanding the FARC’s international distribution routes, and appointing members within each Front to be in charge of coca production. The press release states that the FARC leadership, recognizing that the FARC could not survive without drug revenue, directed its members to disrupt coca fumigation efforts, shoot down fumigation aircraft, and attack Colombian infrastructure to force the government to divert its resources from fumigation. In addition, the leaders ordered FARC members to kidnap and murder US citizens in order to dissuade the United States from fumigating coca and disrupting the FARC’s cocaine manufacturing and distribution activities. In late 2001 and early 2002, FARC leaders participated in a meeting at which they voted unanimously to encourage the kidnapping of US citizens for that purpose. They also called on the FARC to increase cocaine exports to the United States (see Figure 12.1).

Figure 12.1 ▶ Chronology of Key Events in Colombia

Date	Event
1958	Conservatives and liberals agree to form the National Front in a bid to end a civil war that has caused more than two hundred thousand deaths.
1965	National Liberation Army (ELN) and Maoist People's Liberation Army (EPL) are founded.
1966	Revolutionary Armed Forces of Colombia (FARC) is founded.
1971	Left-wing M-19 movement emerges.
1978	President Julio César Turbay (liberal) begins intensive fight against the drug traffickers.
1982	President Belisario Betancur (conservative) grants guerrillas amnesty and frees political prisoners.
1985	M-19 guerrillas kill eleven judges and ninety other people in attack on Palace of Justice.
1989	M-19 becomes legal party after concluding peace agreement.

Figure 12.1 ▶ Chronology of Key Events in Colombia (Continued)

Date	Event
1993	Medellin drug cartel leader Pablo Escobar killed while trying to evade arrest.
1998	President Andres Pastrana (conservative) initiates peace talks with guerrillas, grants the FARC safe haven in the <i>despeje</i> , an area in the southeast the size of Switzerland.
1999	The FARC kills three US Indian rights activists kidnapped in Colombia.
January 1999	Pastrana and FARC leader Manuel "Sureshot" Marulanda meet.
July 2000	Pastrana and the United States launch Plan Colombia with nearly \$1 billion in aid.
April 2001	A report issued by the US House of Representatives Committee on International Relations notes that fifteen IRA members traveled to Colombia over three years to provide military training to the FARC in return for \$2 million in drug money.
October 2001	Pastrana and the FARC sign the San Francisco agreement, committing to negotiate a cease-fire and extend life of the <i>despeje</i> until January 2002.
August 2001	A FARC insurgent and two IRA urban warfare specialists are arrested with explosives in their possession; three more IRA members are arrested and charged with training FARC guerrillas to make bombs.
January 2002	Pastrana accepts the FARC's cease-fire timetable and extends safe haven to April.
February 2002	Pastrana breaks off three years of peace talks following an aircraft hijacking and orders rebels out of safe haven.
May 2002	The FARC kills 119 civilians in the Choco Department using <i>rompas</i> , homemade propane gas mortars.
August 2002	The FARC attacks rock Bogotá as President Alvaro Uribe (Independent) is sworn in; Uribe promises to crack down hard on insurgents.
June 2004	Uribe launches the "Patriot Plan" and deploys fifteen thousand troops to search for and capture the FARC leadership.
May 2006	President Uribe wins second term in office.
June 2007	Colombian government releases dozens of jailed FARC guerrillas to spur a dialogue, but the FARC rejects move.
September 2007	Venezuelan President Hugo Chávez in his role as mediator invites the FARC for talks on a possible hostage release deal.
November 2007	Chávez withdraws his country's ambassador to Bogotá in a row over his role in negotiations between the FARC and Colombian government.

Figure 12.1 ▶ (Continued)

Date	Event
January 2008	The FARC agrees to release two high-profile hostages as part of Chávez mediation.
March 2008	Colombian cross-border strike into Ecuador results in death of senior FARC rebel leader Raul Reyes and sparks diplomatic crisis with both Ecuador and Venezuela.
May 2008	The FARC announces the death of its leader and founder, Manuel Marulanda.
July 2008	Colombian Army rescues highest-profile hostage, Ingrid Betancourt, held in captivity for six years.
February 2009	The FARC releases six high-profile hostages, including former provincial governor.
February 2009	Syrian arms dealer Monzer al-Kassar is sentenced to thirty years in prison for trying to sell surface-to-air missiles, grenades, assault rifles, and C-4 explosives to the FARC for a profit of more than \$1 million.
March 2009	The FARC releases a Swedish man, Erik Larsson, thought to be the last foreign hostage.
March 2009	President Uribe offers peace talks if the FARC halts criminal activities.
August 2009	Relations with Venezuela deteriorate; Venezuela withdraws its ambassador after Colombia accuses it of supplying arms to the FARC.
October 2009	Colombia signs deal with US military giving United States access to seven Colombian military bases.
November 2009	Venezuelan President Chávez orders fifteen thousand troops to the Colombian border and urges his armed forces to prepare for war.
December 2009	The FARC and the ELN announce they will stop fighting each other and concentrate on attacking the Colombian military.
December 2009	The FARC kills the governor of the southern state of Caquetá after abducting him.
March 2010	Spain's High Court says Venezuela facilitated contacts between the FARC and Spain's ETA terrorists and that the FARC had asked the ETA for logistical help with an attempted assassination attempt on Colombian officials visiting Spain.

The Role of US Military Support

Although the FARC has sustained itself as a potent insurgent threat for decades in Colombia, the loss of many of its key leaders and the Uribe administration's aggressive military tactics have taken their toll on the FARC's overall capabilities. US military support to the Colombian armed forces has contributed to the Colombian military's success. The US military supports counterdrug operations from several bases in the United States, most notably US Southern Command in Miami, Florida (see Table 12.1).¹⁵ It also has forces assigned to seven Colombian military bases.¹⁶ US Southern Command assistance to Colombia's armed forces, for example, has included the following:¹⁷

- ▶ Training and equipping elite units
- ▶ Assisting in joint operations
- ▶ Providing training teams to work with Colombian military commanders and their staffs to improve their operational planning
- ▶ Supplying helicopters, intelligence platforms, rations, fuel, and munitions to Colombian military units engaged in operations against high-ranking insurgent leaders

- ▶ Aiding social and civic support programs in communities previously controlled by guerrilla groups

Table 12.1 ▶ US Military Support to Colombia

Key US Military Bases That Support Counterdrug Operations in Colombia
US Southern Command (USSOUTHCOM), Miami, Florida
Joint Interagency Task Force–South (JIATF–South), Key West, Florida
US Army South (USARSO), Fort Sam Houston, Texas
12th Air Force Southern (AFSOUTH), Davis–Monthan Air Force Base, Arizona
Special Operations Command South (USSOCSOUTH), Homestead Air Reserve Base, Miami, Florida

This mutually beneficial relationship has allowed both countries to pursue important objectives; for the Colombians, it has allowed them to pursue guerrilla forces far more aggressively throughout the country and, for the United States, it has helped stem the flow of cocaine from the Andes. But the growing success of US and Colombian military and intelligence operations against the FARC could come at a price of more aggressive and desperate actions by the FARC. The FARC prides itself on being one of the most long-lived insurgencies in South America, and it is well financed through extensive networks that stretch far beyond the Andes. For US decision makers, a key question is whether they can say confidently that war with the FARC is slowly but steadily being won. Or should they be concerned that the FARC might decide out of necessity that it must shift the battlefield and target US interests more directly, both in Colombia and, possibly, within the United States?

RECOMMENDED READINGS

- Brittain, James J. *Revolutionary Social Change in Colombia: The Origin and Direction of the FARC-EP*. London: Pluto Press.
- Gonsalves, Mark, Tom Howes, Keith Stansell, and Gary Brozek. *Out of Captivity: Surviving 1,967 Days in the Colombian Jungle*. New York: HarperCollins, 2010.
- Kirk, Robin. *More Terrible Than Death: Drugs, Violence, and America's War in Colombia*. New York: PublicAffairs, 2003.

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

COLOMBIA'S FARC ATTACKS THE US HOMELAND

Structured Analytic Techniques in Action

Although no analyst has a crystal ball, it is incumbent upon analysts to help 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 taking shape. Red Hat Analysis, Multiple Scenarios Generation, Indicators, and Indicators Validator™ can help analysts accomplish each of these tasks. The fictional “Future Scenario” (Box 12.1) augments the fact-based case study by providing additional narrative to set the stage for employing the techniques.

Box 12.1 TENSIONS MOUNT: A FUTURE SCENARIO

With momentum increasingly on their side, Colombian military commanders and their US advisors decide to launch a combined major offensive against one of the FARC's most important military fronts. After six months of intense planning, a coordinated attack against the FARC's Third Front begins, and most major combat operations are concluded within two weeks. The attack is heralded as a major success: the Third Front's military commander is killed, at least a thousand FARC insurgents are killed or captured, and two members of the FARC's seven-member political Secretariat are captured. Experts are quoted in the press saying the attack might be a tipping point presaging the final demise of the insurgency.

The captured Secretariat members had been indicted previously by the US attorney in Miami on cocaine importation conspiracy charges. Four weeks after the military operation, the Colombian government agrees to extradite both Secretariat members to Miami to face prosecution in US courts.

In Colombia, the remaining members of the Secretariat announce that their movement has suffered major losses but will regroup and live to fight another day “even more deeply committed to the revolutionary struggle.” Their public statements are particularly critical of the role played by US military forces in supporting the operation. The FARC posting on the Internet states, “If the United States is determined to bring the fight to us, then we have

no choice but to bring it to them. There is a price that all American soldiers—and even their friends and families—now must pay for intervening in the internal affairs of Colombia.”

US intelligence learns that in internal deliberations, the FARC leadership is concerned that the attacks are seriously eroding morale within the movement. Moreover, US counterdrug initiatives aimed at the FARC and Colombia are doing serious damage to their drug production, export, and distribution infrastructure. They are overheard saying, “If they go after our infrastructure, then we must go after theirs.” Intelligence analysts interpret this and other statements as indicative of the FARC’s intent to launch a spectacular, retaliatory attack against US persons and places within the borders of the United States.

Technique 1: Red Hat Analysis and Structured Brainstorming

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 the 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.

Brainstorming is a group process that follows specific rules and procedures designed to generate new ideas and concepts. (See Box 12.2.) 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.

Box 12.2 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 discuss 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).

Structured Brainstorming is a systematic 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.

Red Hat Analysis is a reframing technique that requires the analyst to adopt—and make decisions consonant with—the culture of a foreign leader, cohesive group, criminal, or competitor. This conscious effort to imagine the situation as the target perceives it helps the analyst 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 a leader who must make a difficult decision within that operational culture. This reframing process often introduces new and different stimuli that might not have been factored into a traditional analysis. Red Hat Analysis is a useful technique, but the technique alone is of limited value without significant cultural understanding of the other country and people involved.

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.

- 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.
- 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: 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.
- 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.

- 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.
- 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.
- STEP 8:** When all sticky notes have been arranged, ask the group to select a word or phrase that best describes each grouping.
- 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 than 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.
- 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?
- 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.

Analytic Value Added. Were we careful to avoid mirror imaging when we put ourselves “in the shoes” of the FARC Secretariat? Did we explore all the possible forces and factors that could influence how the FARC might launch an attack on the US homeland? 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? Did the labels we generated for each group accurately capture the essence of that set of sticky notes?

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 predictable. 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.

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.

STEP 3: For each of these key drivers, define the two ends of the spectrum.

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.

STEP 5: Develop a story or two for each quadrant of each 2×2 matrix.

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.

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.

Analytic Value Added. Did the technique help us generate a robust set of potential scenarios to consider? Did we discover new scenarios that we probably would not have imagined if we had not used this particular technique? Did similar themes emerge from different matrices even though different pairs of drivers were being considered? Were the final scenarios selected both plausible and the most deserving of attention?

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.

STEP 2: Review and refine each set of indicators, discarding any that are duplicative within any given scenario and combining those that are similar.

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.

Analytic Value Added. What new or otherwise implicit criteria did the indicators process expose? Do the indicators prompt additional areas for collection?

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 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.¹⁸ 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 and then rank order all the indicators.

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. 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 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.

STEP 8: Once nondiscriminating indicators have been eliminated, regroup the indicators under their home scenario.

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.

Analytic Value Added. Does each scenario have a robust set of highly diagnostic indicators? Do these indicator lists provide useful leads for alerting FBI field offices and state and local fusion centers of plausible, potential emerging threats? 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?

NOTES

1. Stephanie Hanson, "FARC, ELN: Colombia's Left-Wing Guerrillas," Council of Foreign Relations Backgrounder, August 19, 2009, http://www.cfr.org/publication/9272/farc_eln.html.
2. Ibid., 4; Farhan Daredia, "FARC Front Leader Extradited to US" [Department of Justice press release], July 17, 2009, <http://www.mainjustice.com/2009/07/17/farc-front-leader-extradited-to-us/>.
3. US Department of the Treasury, "Designation of FARC International Commission Members" [press release], September 30, 2008, <http://www.america.gov/st/texttrans-english/2008/October/20081002123000eaifas0.7901575.html>; Eric Green, "FARC Terrorist Group in Colombia Diminished but Still Dangerous," October 2, 2008, <http://www.america.gov/st/democracy-english/2008/October/200810021603451xeneerg0.7314112.html>.
4. Hanson, "FARC, ELN."
5. Simon Romero, "Manuel Marulanda, Top Commander of Colombia's Largest Guerrilla Group, Is Dead," *New York Times*, May 26, 2008, <http://www.nytimes.com/2008/05/26/world/americas/26marulanda.html>.
6. Simon Romero, "Venezuela Still Aids Colombia Rebels, New Material Shows," *New York Times*, August 2, 2009, <http://www.nytimes.com/2009/08/03/world/americas/03venez.html>.
7. Hanson, "FARC, ELN."
8. Agence France Press, "Spain Charges Thirteen over ETA-FARC Plot to Kill Colombian President," Expatica.com, March 1, 2010, http://www.expatica.com/es/news/spanish-rss-news/spain-charges-19-over-eta-farc-plot-to-kill-colombian-president_27346.html.
9. Warren Hoge, "Adams Delays Testifying in US about IRA Action in Colombia," *New York Times*, April 24, 2002, <http://www.nytimes.com/2002/04/24/world/adams-delays-testifying-in-us-about-ira-action-in-colombia.html>.
10. International Crisis Group, "Colombia: Making Military Progress Pay Off," Latin America Briefing no. 17, April 29, 2008, http://www.crisisgroup.org/~media/Files/latin-america/colombia/b17_colombia_making_military_progress_pay_off.ashx.
11. Ibid.
12. Ibid., 8.
13. MainJustice: Just Anti-Corruption, "FARC Front Leader Extradited to US" [Department of Justice press release], July 17, 2009, <http://www.mainjustice.com/2009/07/17/farc-front-leader-extradited-to-us/>.
14. Hanson, "FARC, ELN."
15. United States Southern Command website, <http://www.southcom.mil/AppsSC/pages/team.php>.
16. "Supplemental Agreement for Cooperation and Technical Assistance in Defense and Security between the Governments of the United States of America and the Republic of Colombia," March 11, 2009, <http://justf.org/content/supplemental-agreement-cooperation-and-technical-assistance-defense-and-security-between-gov>.
17. United States Southern Command, "Fact Sheet: SOUTHCOM Support to Colombia," <http://www.southcom.mil/AppsSC/factFiles.php?id=35>.
18. For a full explanation of Analysis of Competing Hypotheses, see Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, 2nd ed. (Washington, DC: CQ Press, 2015), 181.

13 Understanding Revolutionary Organization 17 November

By Georgia Holmer

Key Questions

- ▶ What was Revolutionary Organization 17 November (17N)?
- ▶ Why is understanding the nature of the group important?
- ▶ What threat did the group pose to US officials in Greece? To others?
- ▶ How might analysts anticipate potential threats from 17N?

CASE NARRATIVE

The Debut

Richard Skeffington Welch and his wife, Christina, had just returned from a Christmas party at the home of the ambassador of the US Embassy in Athens on the evening of 23 December 1975. Welch was a forty-six-year-old veteran intelligence officer and Harvard classics scholar, who was well liked and well suited to his role of chief of station for the Central Intelligence Agency (CIA).¹

As their driver steered the car toward the gated residence in an affluent Athens suburb, Welch himself got out to unlatch the entrance to the driveway. No one in the car had noticed the two young men waiting nearby in the shadows. The taller of the two men approached the American. “Welch!” he demanded. Just as Welch turned to the sound, the man fired a .45-caliber handgun, wounding him fatally. The men ran to a nearby car and escaped, leaving both Mrs. Welch and the driver in a state of horrified shock. Neither was able to provide any details of value to the police; the attack happened quickly and unexpectedly, and it was dark. There were no other witnesses and no significant evidence except for the bullets left in Welch’s body.

The first viable clue was sent to the Greek press in the form of a claim letter signed by the yet unheard-of group “Revolutionary Organization 17 November.” The Greek police, however, had dismissed the “proclamation” as a hoax and issued a ban on publication of the document. It portrayed the document as interference by members of the Greek far left and far right seeking to capitalize politically on the publicity surrounding the murder of an American official.² The Greek tabloids were full of articles accusing the United States, and specifically the CIA, of murdering one of their own. The ban infuriated the group. It then issued a second proclamation accusing the police of incompetence and providing the location of the abandoned getaway car.

INVESTIGADOR_Z



Richard Welch's photograph circulated by the Greek police during the investigation.

Welch's murder took place in a climate of political instability and extreme anti-Americanism in Greece. It had been only a year and a half since the end of the military dictatorship, a rule that succeeded decades of civil conflict, and Greek society was deeply polarized and traumatized.³ Although the junta was bloodless in its ascendancy, its tenure was not. Its repressive tactics were most emblematically and publicly displayed by the events of 17 November 1973. On that date, students at the Athens Polytechnic University staged a large demonstration—the culmination of a series of protests that had grown in scope and vigor over a weeklong period—against the junta. The Greek government responded violently, with numerous police troops backed by army tanks. The clash resulted in the death of at least twenty people⁴ and provoked an international outcry. The event contributed in large part to the destabilization of the military regime, as well as to the radicalization of a number of politicized Greek university students.



Military tanks roll into Athens, 17 November 1973.

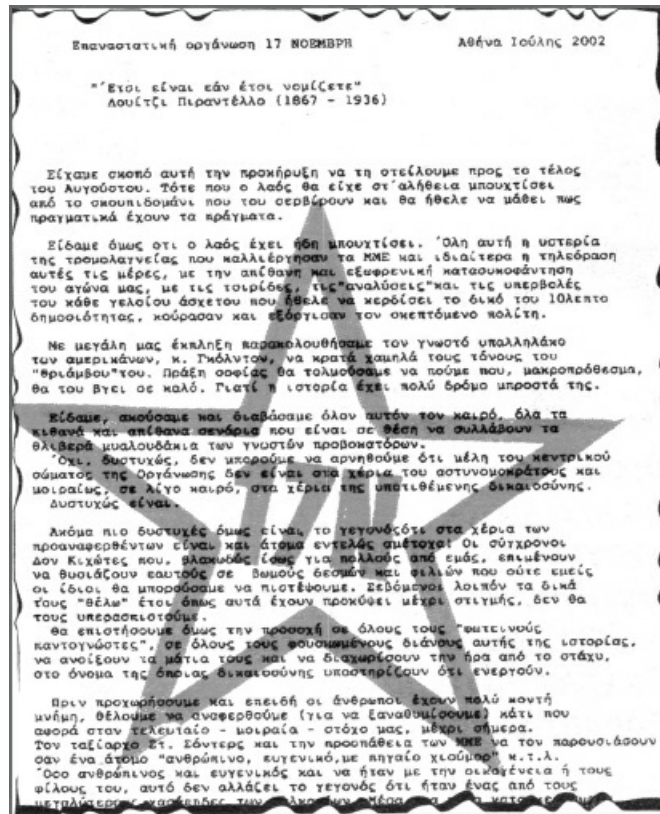
Before his murder, Welch had been identified as the CIA's chief of station in Athens in a

series of articles in the Greek leftist press.⁵ These articles had shared not only Welch's name and assignment but also his home address and telephone number, in case a Greek national wished to contact him directly to discuss the accusations of CIA involvement in Greek domestic affairs. Antipathetic as the environment was, the anger directed at the United States had, until Welch's death, presented more of a nuisance to US officials in Greece than any true danger. US officers routinely had their cars vandalized and firebombed, and the US Embassy and Consulate were subject to destructive demonstrations, but no US officials had been seriously injured. No one anticipated that Welch would become the victim of a politically motivated murder any more than anyone was able to predict, after the crime, that his death would become part of a larger organized campaign that spanned decades and claimed many more lives.

Three Decades of Violence

One year after murdering Richard Welch, 17N shot and killed junta-era military police officer Evangelos Mallios. The shooters used the same .45-caliber handgun that killed Welch and issued a proclamation that echoed the previous communications in tone, voice, and grievance.⁶ These details convinced authorities that Welch's murder was not an isolated event. Mallios's murder also afforded 17N some attention internationally, when the French newspaper *Liberation*, concluding that the police ballistics report linking the weapon to both crimes had established the group's authenticity, then published one of the 17N communiqués on the Welch murder.⁷

17N issued a lengthy ideological treatise in 1977 outlining its Marxist ideology and objective to inspire a popular revolution by targeting individuals whom it perceived as symbols of foreign exploitation and domestic corruption in Greece. Yet it did not strike again until 1980, when members murdered Pantelis Petrou, the deputy commander of the Greek police Riot Control Unit and his driver, Sotiris Stamoulis. The group used the .45-caliber handgun again, now its "signature weapon," ensuring that no other group would claim credit for its attacks and furthering its popular image as revolutionary militants seeking justice for the crimes of the right.⁸ As in the previous attacks, the shooting left little physical evidence and witnesses were scarce.



17N-typed proclamations claimed attacks and articulated grievances and a radical Marxist ideology.

The political rise of Andreas Papandreou and the formation of his Panhellenic Socialist Movement (PASOK) represented a significant period of change for the leftist community in Greece, some of whom abandoned their more radical ideologies and put their hope in the redemption of Greece through PASOK's socialist agenda.⁹ It was assumed that 17N had been a feature of the instability of the immediate post-junta period, and many hoped that its members had entered the political mainstream or at least that the group had lost its impetus as the Greek political system matured. Indeed, it was with some surprise when, on 15 November 1983, 17N operatives shot and killed US Navy Captain George Tsantes and his driver, Nikos Veloutsos, en route to work at the Joint United States Military Advisory Group (JUSMAG). Helmeted men on a motorcycle approached Tsantes's car, shot through the window, and escaped into heavy traffic and the labyrinth of urban Athens.

In its proclamation, 17N expressed its sense of betrayal over PASOK's watered-down version of socialism and seemed particularly chafed by Papandreou's move toward European Community (EC) integration and increased North American Treaty Organization (NATO) ties. The group warned that all CIA, Defense Intelligence Agency (DIA), JUSMAG agents, embassy officials, and US base commanders would be targeted without warning and that drivers and bodyguards were fair game. The proclamation expressed a renewed commitment to "dynamic mass struggle and justified popular revolutionary violence," moving on from the crimes of the junta era and focusing on the current state of affairs in Greece.¹⁰ The targets during the next five years would continue to be representatives of the Greek political establishment and "agents of

US imperialism.”

17N attempted another motorcycle assassination attack in April 1984, this time against US Army Master Sergeant Robert Judd on his mail delivery run, but Judd survived through quick-witted defensive driving. He jumped a median on a major thoroughfare and drove himself directly to the hospital to be treated for his injuries. In February 1985, 17N shot and killed Nikos Momferatos, the publisher of Greece’s largest conservative paper, *Apogevmatini* (literally, “the Afternoon”), together with his driver, accusing Momferatos of being an agent of the CIA.¹¹

An attack in November 1985 demonstrated a new level of tactical sophistication on the part of the group and a certain escalation in the campaign. 17N detonated a remote-controlled bomb against a Greek Monades Apokatastasis Taksis (MAT; “Units for the Reinstatement of Order”) riot police bus, and many police officers were seriously injured and one killed. This was a period of intense terrorist activity in Europe, not only from indigenous European violent left-wing groups such as the Baader-Meinhof Gang or Red Army Faction in Germany and the Red Brigades in Italy, but also from spillover terrorism from the Middle East, especially radical Palestinian groups. It was the heyday of Carlos the Jackal, Abu Nidal, and other terrorists, many of whom used Greece as a theater of operations. It was also a period of cross-pollination of ideologies and resources among many groups and individuals.¹² The 1985 bombing attacks by 17N did not look like the group’s usual modus operandi. Previous 17N attacks had involved a motorcycle or getaway car, a couple of handguns, and a reliance on the limitations of the investigative prowess of the Greek police.

This new style of attack for 17N augmented but did not replace the shooting attacks, however. In 1986, 17N shot and killed leading Greek industrialist Dimitris Angelopoulos, the chair of the Halivourgiki steel company and close friend of Papandreou. Angelopoulos’s company accounted for 60 percent of Greece’s steel production. In its proclamation claiming the attack, 17N accused Angelopoulos of smuggling his profits to his accounts in the United Kingdom, leaving his Greek business to flounder.¹³ As it would in later proclamations claiming attacks against other prominent and politically tied Greek businesspeople, 17N seemed deeply concerned with and knowledgeable about the details of financial wrongdoing and corruption.

The frequency of attacks by 17N continued to increase. Two separate, remotely detonated bombs targeted military transport buses ferrying US servicemembers across Attica in 1987; there were minor injuries but no deaths. In 1988, a 17N operative placed a bomb in the trashcan outside the residence of Drug Enforcement Administration (DEA) agent George Carros, but aborted the operation when the device failed to detonate.¹⁴ The group returned to its tried-and-true method of motorcycle drive-by assassinations with the murder of Greek businessman Alexandros Athanasiades in March of that year. Athanasiades was the general director of a major mining company and of Greece’s largest arms company. Like Angelopoulos, 17N accused him of corruption and membership in the “lumpen big bourgeois class.”¹⁵



Photograph attached to a 17N proclamation that shows pictures of Karl Marx, Che Guevara, and Aris Velouchiotis, a Greek communist fighter; the 17N logo on a flag; and stolen weaponry.

A few months later, 17N carried out an attack that would garner world attention. On 28 June 1988, 17N detonated a powerful car bomb, killing the US military attaché in Athens, Navy Captain William Nordeen, as his vehicle passed en route to work. The explosion, shaped by piles of cement bags, hurled Nordeen's body more than fifty feet away. In the ensuing proclamation, 17N claimed, "We decided to execute a senior official of US imperialism's military forces in our country," and went on to blame the United States for recent Greek-Turkish airspace skirmishes and perceived Turkish territorial incursions.¹⁶

Later that same year, 17N members staged a siege of an Athens suburban police station. Without firing a single bullet, they stole a number of weapons and police paraphernalia. A 17N communiqué included a photo of the group's newly looted cache in front of its group symbol—a red 17N inside a yellow five-pointed star—alongside portraits of Karl Marx and Aris Velouchiotis, a famous Greek communist fighter. 17N also began conducting kneecappings, wounding physicians and two public prosecutors—including one who bled to death during incompetent medical treatment—for collusion with a corrupt system.

In May 1989, 17N attempted a repeat of the Nordeen attack, this time targeting former Greek Minister of Public Order Giorgios Petsos. The timing of the attack was off, however, and the minister and his driver survived. As was the case with unsuccessful bombings in the past, 17N followed up with a return to its signature gun. Four months later, the group shot and fatally wounded Pavlos Bakoyiannis, the chief parliamentary spokesperson of the conservative New Democracy (ND) Party and son-in-law of ND leader Konstantinos Mitsotakis. The attack occurred the same day that Papandreou and several of his former ministers were to stand trial on bribery charges.¹⁷ Such timing gave rise to conspiracy theories of government collusion in 17N, a theme that had recurred in less reputable Greek press reports for years.

The resulting increased focus on 17N met with yet another escalation in violence and a new tactical approach. On 5 February 1990, 17N brazenly walked into the National War Museum in Athens in broad daylight and stole two bazookas from a display. In an ensuing communication, it

also admitted to stealing weaponry—a collection of rockets, grenades, and explosives—from a military warehouse in Larissa (several hours north of Athens). Proof of the cache came in the form of an accompanying photo. 17N would go on to use these stolen rockets and explosives against a range of targets during the next few years, demonstrating an incoherent broadening of grievances and causing a huge amount of property damage. Bombs were exploded against vehicles, homes, and businesses belonging to Greeks, Turks, Americans, British, French, and Germans. Using makeshift PVC pipes as launchers, rockets were fired against a British Petroleum office, a major Greek hotel, the Greek power company, police buses, a Greek cement plant, and the German companies Siemens and Lowenbrau. 17N even tried—unsuccessfully—to target individuals with the rockets: Greek shipping tycoon Vardis Vardinoyiannis in 1990 and Financial Minister Ioannis Paliokrassas in 1992. In the latter attack, instead of the intended target, shrapnel from the rocket killed a university student who was passing by the scene.¹⁸

1991 was 17N’s bloodiest year. 17N killed four people: two Turkish diplomats; a Greek police officer; and, using a massive remote-controlled bomb, a US Air Force sergeant. In November 1991, there was a shoot-out between police and 17N operatives in the Athens neighborhood of Sepolia, and Greek police officers were overwhelmed. After a period of quiet, the group reemerged in 1994 with a return to close-range assassinations using the signature handguns. That year, 17N operatives shot and killed the former National Bank of Greece Governor Michalis Vranopoulos and a Turkish diplomat, Omar Sipohioglu. In 1997, it ambushed and murdered Greek shipowner Constantinos Peratikos. With the group no longer cast as revolutionary heroes and having lost the majority of its popular support, the 17N attack was received with sadness and dismay by the Greeks. The more mainstream media focused on lambasting the Greek police for their inability to apprehend the group members. Accusations of Greek police ineptitude were heightened by the discovery that the battery on the 17N operatives’ getaway car had given out and that the attackers had been forced to escape on foot and then commandeer a taxi cab, creating what seemed like ample opportunity to apprehend them.¹⁹

By 1999, many wondered whether 17N had run its course. Its message had lost its relevance and its attacks had become less frequent. Increased US Embassy security measures had helped make American officials hard targets. The US Embassy had one of the highest levels of physical security and executive protection in the world, and one of the largest diplomatic security budgets.²⁰ Other than nonlethal bombings against American businesses such as Citibank, and an unimpressive firing of a rocket against the rear wall of the US Embassy in 1996, 17N had not struck an American since the murder of the Air Force sergeant in 1990.

Almost everyone was shocked on 8 June 2000, when two helmeted men shot and killed the British Embassy military attaché in Athens, Brigadier Stephen Saunders. The attack was reminiscent of the drive-by motorcycle shootings of Tsantes and Athanasiades in the 1980s. It was in heavy morning rush-hour traffic at almost the exact same point on Kiffisas Avenue, a major thoroughfare in Athens, where 17N had pulled off other successful, similarly styled assassinations. With this killing, 17N had launched more than thirty significant attacks against US and other targets over a twenty-five-year period (see Table 13.1).

Table 13.1 ▶ Timeline of Significant 17N Attacks ²¹	

1975	Richard Welch, CIA chief of station in Athens, killed (shot)	American
1976	Evangelos Mallios, Greek military police officer, killed (shot)	Greek
1980	Pantelis Petrou, deputy commander of Greek Riot Squad (MAT), and his driver, Sotiris Stamoulis, killed (shot)	Greek/Greek
1983	George Tsantes, US Navy captain and his driver, Nikos Veloutsos, both killed (shot)	American/ Greek
1984	Robert Judd, US Army master sergeant, attempted murder (shooting)	American

Table 13.1 ▶ Timeline of Significant 17N Attacks²¹ (Continued)

	Christos Matis, Greek police officer, killed during a 17N bank robbery (shot)	Greek
1985	Nikos Momferatos, newspaper publisher, and Georgios Roussetis, his driver, both killed (shot)	Greek/Greek
	Bombing of Greek MAT bus, one killed, others injured	Greek
1986	Dimitris Angelopoulos, chair of Halivourgiki steel company, killed (shot)	Greek
1987	Zacharias Kapsalakis, neurosurgeon, kneecapped	Greek
	Bombing of a transport bus carrying US servicemembers (April), injuries	American
	Bombing of a transport bus carrying US servicemembers (August), injuries	American
1988	George Carros, DEA agent, attempted murder (bombing)	American
	Alexandros Athanasiades, industrialist, killed (shot)	Greek
	William Nordeen, US Navy captain, killed (car bomb)	American
1989	Constantinos Androulidakis, public prosecutor, intended kneecapping but victim dies of complications	Greek
	Panayiotis Tarasouleas, public prosecutor, kneecapping	Greek
	Giorgios Petsos, minister of public order, attempted murder (car bomb)	Greek
	Pavlos Bakoyiannis, New Democracy chief parliamentary spokesperson, killed (shot)	Greek
1990	Vardis Vardinoyiannis, shipping tycoon, attempted murder (rocket attack)	Greek
1991	Ronald Stewart, US Air Force sergeant, killed (bomb)	American
	Deniz Bouloukbasi, Turkish chargé d'affaires, attempted murder (bomb)	Turkish
	Cetin Gorgu, Turkish Embassy press attaché, killed (shot)	Turkish
	Rocket attacks against Greek MAT bus, one officer killed, others injured	Greek

Table 13.1 ▶ (Continued)

1992	Ioannis Palaokrassas, financial minister, attempted murder (rocket attack); passerby (Athanasios Axarlian) killed	Greek
	Eleftherios Papadimitriou, New Democracy member of the parliament, kneecapping	Greek
1994	Michalis Vranopoulos, former National Bank of Greece governor, killed (shot)	Greek
	Omar Sipahioglu, Turkish diplomat, killed (shot)	Turkish
1996	Rocket attack against US Embassy, no injuries	American
1997	Constantinos Peratikos, shipowner, killed (shot)	Greek
2000	Stephen Saunders, British military attaché, killed (shot)	British

Athens had been awarded the Olympics Games for 2004, and with growing international scrutiny, the Greek police were under great pressure to respond effectively to the next opportunity to disrupt the group. The questions remained: Who was 17 November? What threat did it pose? To whom? And how?

RECOMMENDED READINGS

Kassimeris, George. *Europe's Last Red Terrorists*. London: Hurst & Company, 2001.

Kassimeris, George. "Fighting for Revolution? The Life and Death of Greece's Revolutionary Organization 17 November, 1975–2002." *Journal of Southern Europe and the Balkans* 6, no. 3 (2004): 259–73.

Kiesling, Brady. *Greek Urban Warriors: Resistance and Terrorism 1967–2012*. Athens: Lycabettus Press (forthcoming in 2014).

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

UNDERSTANDING REVOLUTIONARY ORGANIZATION 17 NOVEMBER

Structured Analytic Techniques in Action

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: 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.

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.

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

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

STEP 5: Update the list of alternative hypotheses.

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

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

Analytic Value Added. Did using the technique help you challenge conventional wisdom about the group and its motives? Did it reveal ideas or concepts that you might have missed if you had engaged in conventional brainstorming only? Was it difficult to select those hypotheses that deserved the most attention?

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.

STEP 3: Generate a list of indicators for each scenario that would point to the events starting to play out.

STEP 4: Assess the level of damage or disruption that would result from each scenario and how difficult it would be to overcome.

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.

Analytic Value Added. Did the technique help you generate new ways of thinking about the problem? Did it help you assess how difficult each scenario would be to carry out? Did the exercise indicate that any new security measures should be implemented?

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.
9. Foreign government penetrates database to download corporate data.
10. 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.

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 (a sample template is provided in Table 13.3).

Table 13.3 ▶ Foresight Quadrant Crunching™ Template

Key Component	Contrary Assumption	Contrary Dimensions
Who?		
What?		
How?		
When?		
Where?		
Why?		

STEP 5: Array combinations of these contrary assumptions in sets of 2×2 matrices.

STEP 6: Generate one or two credible scenarios for each quadrant.

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.

Analytic Value Added. Which scenario is the most deserving of attention? Should attention focus on just one scenario, or could several scenarios play out simultaneously? Are any key themes present when reviewing the most likely set of attention-deserving scenarios? Does this technique help you determine where to devote the most attention in trying to deter an attack? Does it help you challenge any key assumptions regarding how an attack might take place?

NOTES

1. "U.S. Aide Is Killed in Greece," *Washington Post*, December 24, 1975, 1.
2. George Kassimeris, *Europe's Last Red Terrorists* (London: Hurst, 2001), 73.
3. C. M. Woodhouse, *Modern Greece: A Short History* (London: Faber and Faber, 1991), 310.
4. *Ibid.*, 313.
5. Rhodri Jeffrey-Jones, *In Spies We Trust: The Story of Western Intelligence* (Oxford: Oxford University Press, 2013), 168.
6. Kassimeris, *Europe's Last Red Terrorists*, 74–75.
7. *Ibid.*
8. *Ibid.*, 75.
9. Woodhouse, *Modern Greece*, 313; and Kassimeris, *Europe's Last Red Terrorists*, 75.
10. Kassimeris, *Europe's Last Red Terrorists*, 76.
11. *Ibid.*, 78.
12. Yonah Alexander and Dennis Pluchinsky, eds., *European Terrorism Today and Tomorrow* (Washington, DC: Brassey's, 1992), 1–29.
13. Kassimeris, *Europe's Last Red Terrorists*, 80.
14. Alexander and Pluchinsky, *European Terrorism*, 102.
15. Kassimeris, *Europe's Last Red Terrorists*, 82.
16. Alexander and Pluchinsky, *European Terrorism*, 103.
17. Kassimeris, *Europe's Last Red Terrorists*, 89.
18. *Ibid.*, 96.
19. *Ibid.*, 102.
20. Paul Pillar, *Terrorism and the United States* (Washington, DC: Brookings Institution Press, 2003), 179.
21. "Chronology of 17 November Attacks," *Kathemerini*, English ed., August 7, 2002.

14 Defending Mumbai from Terrorist Attack

Key Questions

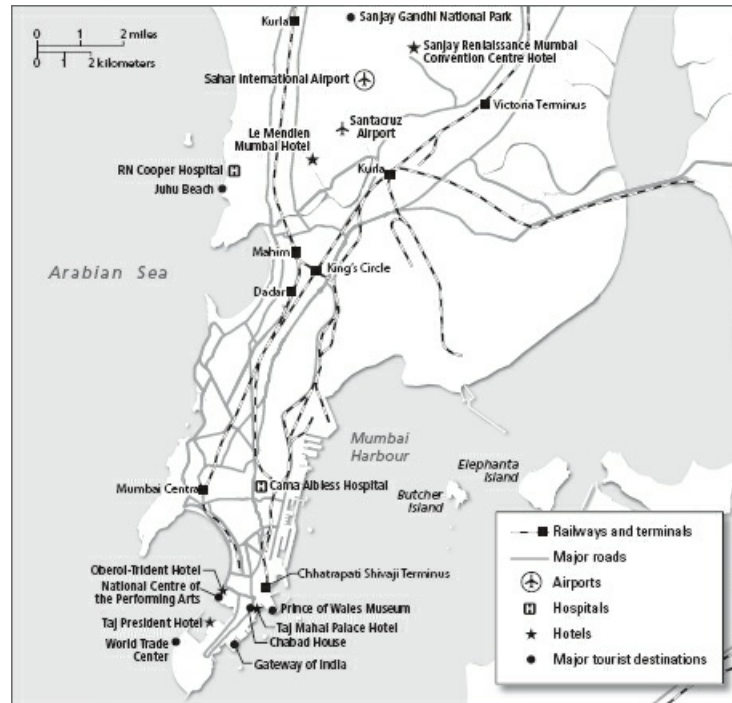
- ▶ What are the most likely terrorist targets in Mumbai?
- ▶ What type of attack would the terrorists most likely mount?
- ▶ How would they gain access to the city?
- ▶ What can be done to deter future terrorist attacks?

CASE NARRATIVE

The teeming sprawl of modern Mumbai's more than 18 million residents had humble beginnings.¹ Poised on a peninsula jutting into the Arabian Sea (see Map 14.1), the city formerly known as Bombay began its life as a small fishing village populated by native Koli people.² Portuguese sailors later claimed the Koli's seven swampy islands but did not see much value in them. In 1661, the Portuguese government gifted the islands to Britain as part of the dowry for Charles II's marriage to Catherine of Braganza. The city's gradual transformation into a bustling hub of world commerce began when the East India Company recognized the potential of the location's natural harbor and leased the islands from the British Crown. The subsequent colonization of India by Britain and the development of the textile industry in the mid-nineteenth century solidified the city's importance to Asia and the rest of the world.

By 2008, Mumbai had become the epicenter of India's booming economy. The city hosts India's stock exchange and boasts a population density four times greater than that of New York City.³ A recent Global Cities Index rated Mumbai as the world's fourth most populous city, with the twenty-fifth highest gross domestic product.⁴ Mumbai's modern docking facilities, rail connections, and international airport make it India's gateway to the world's globalized economy.⁵ The city is also home to the popular Bollywood film industry, which churns out movies whose financial success is eclipsed only by that of their American counterparts. A virtual kaleidoscope of colors and cultures, Mumbai is both a playground for the fantastically wealthy and a congested shantytown for the urban poor. Local residents boast that it is a city that never sleeps, with streets that are never empty.⁶

Map 14.1 ■ Mumbai Peninsula



Source: Pherson Associates, LLC, 2011.

It was not Mumbai's spectacular growth and increasing globalization that was foremost on the minds of Indian security officials in the fall of 2008, however. In mid-October, the United States had quietly told the Indian government that intelligence collected in Pakistan warned of an "oncoming attack that will be launched by terrorists against hotels and business centers in Mumbai (formerly Bombay)."⁷ The source of the warning made it credible, but it lacked specificity about the attackers and their methods, weapons, and targets. Absent such details, it would be difficult to assign priorities in defending the vast city. It fell to Indian intelligence and law enforcement officials to identify the most likely whens, wheres, and hows of an attack.

A History of Violence

Mumbai already had long experience as a target of terrorism. Between 1993 and 2008, terrorists conducted numerous bomb attacks in and around the city (see Table 14.1). Several of the incidents involved simultaneous attacks on multiple targets. In all, 544 died and 1,774 sustained injuries in the attacks. The assailants' weapons of choice included bombs—often hidden or thrown from motor scooters—and grenades. During this period there were no reports of suicide bombings.

The most notable of these attacks occurred in 1993, when Islamic terrorists exploded devices at thirteen locations throughout Mumbai, causing extensive casualties. The targets ranged from hotels to the airport to bazaars. The modus operandi was a staged vehicle with RDX bombs (see Box 14.1, on RDX bombs), although the assailants also threw grenades at some of the targets.⁸ The attack was orchestrated by Dawood Ibrahim, a well-known organized crime leader, in response to ongoing violence between Hindus and Muslims in prior months and, more specifically, as retaliation for the destruction of a sixteenth-century mosque in late 1992.⁹ Hinduism is the dominant religion in India; only 12 percent of the population is Muslim.

Perceived inequities have been a major factor sparking intercommunal violence in the country.

Table 14.1 ► Bomb Blasts in Mumbai, 1993–2008*

Date	Place	Killed	Injured
12 March 1993	Thirteen attacks throughout city	257	700
23 January 1998	Kanjurmarg Station	unknown	unknown
24 January 1998	Goregaon and Malad railway tracks	0	2
27 February 1998	Three bombings at Virar, Santa Cruz, and Kandivali railway stations	9	22
2 December 2002	Bus in Ghatkopar at railway station	3	34
6 December 2002	Air-conditioning vent in McDonald's, central railway station	0	25
27 January 2003	Bicycle near Vile Parle railway station	1	25
13 March 2003	Train car at Mulund Station	10	70
14 April 2003	Parcel at V. N. Jewelers in Bandra	1	0
28 July 2003	Bus in Ghatkopar near a telephone exchange	4	32
25 August 2003	Two taxis at Gateway of India and Zaveri Bazaar	50	150
11 July 2006	Seven trains around the city	209	714
	Total Casualties	544	1,774

*No attacks were recorded in 2007 and 2008.

Box 14.1 RDX BOMBS

RDX, commonly known as cyclonite, was widely used during World War II, often in explosive mixtures with TNT.ⁱ During World War II, the British termed cyclonite “Research Department Explosive” (R.D.X.) for security reasons and used it as a more powerful form of TNT for attacking German U-boats.ⁱⁱ It was one of the first plastic explosives and has been used in many terrorist plots.ⁱⁱⁱ Outside of military applications, RDX is used in controlled demolition to raze structures. Ahmed Ressay, the al-Qaeda “Millenium Bomber,” used a small quantity of RDX as one of the components in the explosives that he prepared to bomb Los Angeles International Airport on New Year’s Eve, 1999–2000; the combined explosives could have produced a blast forty times greater than that of a devastating car bomb.^{iv}

i. Tenney L. Davis, *The Chemistry of Powder and Explosives*, Vol. II (New York: John Wiley & Sons, 1943).

ii. MacDonald and Mack Partnership, *Historic Properties Report: Newport Army Ammunition Plant; Newport Indiana*, AD-A175 818, prepared for National Park Service (Minneapolis, MN: MacDonald and Mack Partnership, 1984), 18, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA175818>.

iii. John Sweetman, *The Dambusters Raid* (London: Cassell Military Paperbacks, 2002), 144.

iv. *US v. Ressay*, US Court of Appeals for the Ninth Circuit (February 2, 2010),

Five years later, a series of bombings occurred at train stations across the city and in the suburbs. Over a two-month period, assailants conducted successful attacks at six different train stations in three separate incidents.¹⁰ The terrorists targeted railway stations, platforms, and tracks. During the trial of the accused men, the prosecutor argued the attack was conducted at the behest of the Pakistani Inter-Services Intelligence (ISI). Some of the blasts occurred the night before parliamentary elections.¹¹

From December 2002 through August 2003, seven violent incidents occurred. Although all the attacks involved bombings, these incidents had the most variation in attack method. In the first attack on 2 December, a bomb was placed on a bus at the Ghatkopar train station.¹² Four days later, a bomb exploded in an air-conditioning vent inside a McDonald's fast-food restaurant at the central railway station.¹³ Roughly a month and a half later, on 27 January, a bomb attached to a bicycle exploded at the Vile Parle train station.¹⁴ About two weeks later, on 13 March, a bomb exploded inside a train car at the Mulund train station.¹⁵ The most unusual attack occurred a month later, on 14 April, when a parcel exploded inside a jeweler's store.¹⁶ No attacks were recorded in May or June, but on 28 July a bus at Ghatkopar train station was destroyed by a bomb.¹⁷ The final and deadliest attack in this series occurred on 25 August. Two taxis exploded at the Gateway of India and at the Zaveri Bazaar, killing 50 people and injuring 150.¹⁸



Wreckage from 25 August 2003 terrorist bombing attacks at Zaveri Bazaar in Mumbai.

Most of the attacks were traced back to radical Islamic groups; most of these were based in Pakistan. Authorities believed the Student Islamic Movement of India (SIMI) was responsible for the 6 December 2002 and 25 August 2003 attacks; Laškar-ě-Taiba (LeT) was suspected in the 25 August 2003 attack as well.¹⁹

Almost three years passed until the next incident, which came to be called 7/11. On 11 July 2006, seven explosions occurred on seven trains along the western rail line in Mumbai between 1824 and 1835 hours.²⁰ The explosions occurred at or near the Khar, Mahim, Matunga,

Jogeshwari, Borivili, and Bhayandra-Mira Road train stations and between the Khar and Santa Cruz stations. Each bomb consisted of a pressure cooker filled with 2.5 kilograms of RDX and ammonium nitrate; the bombs were placed inside first-class train compartments.²¹ Indian officials claimed that SIMI and LeT conducted the attacks on behalf of the Pakistani ISI.²²

Recent Major Terrorist Attacks in India

Mumbai has not been the only target of attack for Muslim and separatist groups. From 2001 to 2008, twenty-one major incidents occurred elsewhere in India (see Map 14.2).²³ Some 550 people died in these attacks, most of which involved bombs.

Assailants used a vehicle-borne improvised explosive device (VBIED) to blow up the front gate of the Jammu and Kashmir state assembly complex on 1 October 2001. Two attackers entered the complex and opened fire until security forces shot and killed them.²⁴ Two months later, on 13 December 2001, five individuals attacked the National Parliament in New Delhi using AK-47s and grenades.²⁵ At least one of the attackers was wearing a suicide vest, but it exploded after he was shot, and it did not harm anyone.²⁶ The terrorist group Jaish-e-Mohammed (JEM) claimed responsibility for the October attack, and some of its members were convicted; authorities also suspected LeT of involvement.²⁷

On 24 September 2002, terrorists launched a similar attack on the Hindu temple complex in Gandhinagar. Two terrorists entered the complex and opened fire with AK-47s; they also threw hand grenades before being killed by Indian commandos.²⁸ Another attack using similar tactics occurred on 14 May 2002, when three attackers fired at a bus and then attacked the Kalu Chak army camp in Jammu.²⁹ LeT was suspected of conducting the attack, and press reports raised the specter of Pakistani support.³⁰

Map 14.2 ■ India, Mumbai, and Previous Attack Sites



Source: Pherson Associates, LLC, 2011.

Sporadic bombings continued for several years.

- ▶ On 15 August 2004, a bomb exploded in Assam during the Independence Day parade.³¹ The attack was attributed to the United Liberation Front of Asom (ULFA),³² a terrorist group with the goal of “establishing a ‘sovereign socialist Assam’ through armed struggle.”³³
- ▶ On 29 October 2005, three bombs exploded during the festival of lights in New Delhi³⁴ at two marketplaces and on a bus.³⁵ Police suspected that a group connected to LeT, called Inquilab, was responsible for the attack.³⁶
- ▶ Terrorists detonated bombs at the Sankat Mochan temple and a train and hall in the Cantonmen railway station in Varanasi on 7 March 2006. The tactics were similar to those used in the Gandhinagar attack, and as many as ten other bombs were found throughout the city.³⁷
- ▶ On 8 September 2006, two or three bicycle bombs exploded at a Muslim graveyard near a mosque just before prayers began on Shab-e-Barat.³⁸ Although it is not clear who was responsible for the attack, one person arrested for the incident had ties to LeT.³⁹

In 2007, the frequency of attacks began to escalate. In the past, nearly all attacks on trains in India had occurred at or near a primary rail station. On 19 February 2007, however, two crude briefcase bombs were detonated on a train near the village of Dewana and set the train on fire. The train was heading to the Pakistani–Indian border when it caught fire. Officials found two unexploded briefcases in other cars on the train. The attack took place the day before scheduled India–Pakistan peace talks began.⁴⁰

Only three months later, on 18 May 2007, a bomb exploded during prayers at the Mecca Masjid in Hyderabad, a city populated mostly by Muslims.⁴¹ In addition to the bomb that detonated, police found two unexploded bombs with cell phone triggers inside the mosque that had failed to explode. Following the blast, Muslim protestors at the site became unruly, and police fired into the crowd, killing some of the protestors.⁴² Hyderabad was the site of violence again when two bombs exploded in the early evening of 25 August 2007. The terrorists targeted the Lumbini Amusement Park and the restaurant Gokul Chat Bhandar.⁴³ Authorities discovered nineteen other bombs hidden throughout the city.⁴⁴

On 11 October, a blast at a Sufi mosque in Ajmer killed three people. A few days later, on 14 October, a theater in Ludhiana was rocked with an explosion that killed seven people. Three simultaneous bombs on 23 November in judicial complexes in Lucknow, Varanasi, and Faizabad killed thirteen.⁴⁵

The number of terrorist attacks escalated even further beginning in May 2008. On 13 May, seven bombs exploded in Jaipur at several markets and Hindu temples. On 25 July 2008, eight bombs exploded in Bengaluru (formerly Bangalore). The next day, sixteen bombs exploded in Ahmedabad. Then, on 13 September, five bombs exploded in the markets of New Delhi. Suspicion for the Jaipur, Bengaluru, and New Delhi attacks fell on SIMI, LeT, and Harkat-ul-Jihad-al-Islami (HUJI), a Sunni terrorist group.⁴⁶ SIMI was also associated with the Ahmedabad attack.⁴⁷ A group called the Indian Mujahideen, however, claimed responsibility for the Jaipur, Ahmedabad, and New Delhi attacks.⁴⁸

Two weeks after the explosions in New Delhi, another bomb went off in the city on 24 September 2008. Two terrorists dropped the bomb in a bag from their motorcycle, and a ten-year-old boy was trying to return it to them when the bomb exploded.⁴⁹ Two days later, in the towns of Modasa and Malegaon, two bombs exploded nearly simultaneously after being dropped from motorcycles.⁵⁰ The attack in Modasa occurred in a Muslim-dominated market.⁵¹ In Malegaon, the blast occurred near a building previously used by SIMI before it was banned.⁵²

Three attacks occurred in the following month. The first occurred in Kanpur when a bomb on a bicycle exploded on 14 October.⁵³ The next attack occurred a week later on 21 October in Imphal. The bomb had been placed on a motor scooter⁵⁴ and may have been targeting a nearby police complex. Authorities suspected a separatist group called the People's Revolutionary Party of Kangleipak, based out of Myanmar (Burma), of conducting the bombing.⁵⁵ The deadliest of the attacks that month occurred on 30 October in Assam. As with the attacks in Jaipur, Ahmedabad, and Bengaluru, and the first New Delhi attack in September 2008, multiple bombs—eighteen—using RDX⁵⁶ exploded throughout the city nearly simultaneously. Authorities suspected HUJI and ULFA of carrying out the attacks.⁵⁷

Countering the Threat

Responsibility for defending Mumbai from terrorist attack is shared by several law enforcement and intelligence organizations at both the local and national levels. At the national level, in addition to military intelligence, two main civilian intelligence services as well as other ministries share an intelligence mandate. At the local level, the police respond to and share information based on national-level guidance regarding terrorist activities.

The Research and Analysis Wing (RAW) and the Intelligence Bureau are the two main civilian intelligence services. The RAW is the country's foreign intelligence unit and focuses

primarily on issues outside India's borders, mostly in the neighboring countries of Pakistan and Bangladesh.⁵⁸ The Intelligence Bureau concentrates primarily on domestic security.⁵⁹ Both services are routinely engaged in collecting intelligence on and assessing the threat posed by militant Pakistani Islamist groups. Along with RAW, the Army's Signals Intelligence Directorate collects signals intelligence that has the potential to reveal terrorist planning and operations.⁶⁰

India's Ministry of Home Affairs has several armed units it can task to assist in internal security matters. The Border Security Force is a paramilitary service dedicated to monitoring the country's international frontiers.⁶¹ The Indian Home Guard is a paramilitary force capable of serving as an auxiliary to the Indian Police Service—a nationwide law enforcement unit. The National Security Guard, also known as the "Black Cats," is a highly trained counterterrorism force capable of preventing or responding to large-scale terror assaults.⁶²

In addition to these national resources, the Mumbai Police Department has had extensive experience trying to counter terrorist attacks. In 2004, the Mumbai Police Department created an elite Anti-Terrorism Squad to exchange information on terrorist threats and coordinate its activities with national intelligence agencies. Members of the squad receive special weapons and tactics training.⁶³

RECOMMENDED READINGS

- Rabasa, Angel, et al. *The Lessons of Mumbai*. Santa Monica, CA: RAND Corporation, 2009.
http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf.
- Rotella, Sebastian. "On the Trail of a Terrorist." *Washington Post*, November 14, 2010.
<http://www.washingtonpost.com/wp-dyn/content/article/2010/11/13/AR2010111304345.html>.

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

DEFENDING MUMBAI FROM TERRORIST ATTACK

Structured Analytic Techniques in Action

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.

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.)

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).

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.

- 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.

Analytic Value Added. Were we careful to avoid mirror imaging when we put ourselves “in the shoes” of Muslim terrorist planners? Did we explore all the possible forces and factors that could influence how the terrorists might gain access to Mumbai to launch their attack? Did we cluster the ideas 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 any new lines of inquiry?

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.

- 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.
- 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.
- 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.
- 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? Did some criteria deserve greater weight than others? Did you reflect this when you rated the various ideas?

Technique 3: Classic Quadrant Crunching™

Classic Quadrant Crunching™ combines the methodology of a Key Assumptions Check⁶⁴ with Multiple Scenarios Generation⁶⁵ 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.

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 (a sample template is provided in Table 14.3).

Table 14.3 ▶ Classic Quadrant Crunching™ Matrix Template		
	Key Components of the Lead Hypothesis	Contrary or Alternative Dimensions

STEP 5: Array combinations of these contrary assumptions in sets of 2×2 matrices.

STEP 6: Generate one or two credible scenarios for each quadrant.

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.

Analytic Value Added. Which scenario is the most deserving of attention? Should attention focus on just one scenario, or could several scenarios play out simultaneously? Are any key themes present when reviewing the most likely set of attention-deserving scenarios? 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?

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.

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, 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.

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? Can the indicators be used to help detect a planned attack or deter a possible hostile course of action?

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.⁶⁶ 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.

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 unlikely ratings. In some cases, an indicator may be worth keeping if it is useful when viewed in combination with several other indicators.

STEP 8: Once nondiscriminating indicators have been eliminated, regroup the indicators under their home scenarios.

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.

Analytic Value Added. Does each scenario have a robust set of highly diagnostic indicators? 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?

NOTES

1. "Introduction to Mumbai" (from *Frommer's India*, 3rd ed.), *New York Times* website, 2009, http://travel.nytimes.com/frommers/travel/guides/asia/india/mumbai/frm_mumbai_3476010001.html.

2. The Municipal Corporation of Greater Mumbai, "Mumbai Travel Guide," <http://www.mcgm.gov.in/irj/portal/anonymous/qlmumbaitravelguide>.
3. "Introduction to Mumbai."
4. "The Global Cities Index," *Foreign Policy* (September/October 2010), 124.
5. "Introduction to Mumbai."
6. The Municipal Corporation of Greater Mumbai."
7. "US Warned India 'Twice' about Sea Attack: Report," *Indian Express*, December 2, 2008, <http://www.indianexpress.com/news/us-warned-india-twice-about-sea-attack-re/393184/>; 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>.
8. Express News Service, "100 Guilty," *Mumbai Newslite*, May 18, 2007, <http://cities.expressindia.com/fullstory.php?newsid=236913>.
9. "'93 Mumbai Blasts: 3 Get Death Sentence," *Times of India*, July 18, 2007, archived at http://web.archive.org/web/20071213221400/http://timesofindia.indiatimes.com/India/93_Mumbai_blasts_3_get_death_sentence/; "Mumbai Bombing Sentencing Delay," *BBC News*, September 13, 2006, http://news.bbc.co.uk/2/hi/south_asia/5340660.stm.
10. "'98 Blasts: Guilty to Be Sentenced on Wednesday," *Times of India*, July 3, 2004, <http://timesofindia.indiatimes.com/articleshow/763146.cms>.
11. "Mumbai's Trains under Attack for More Than a Decade," *Times of India*, March 14, 2003, <http://timesofindia.indiatimes.com/articleshow/40207873.cms>.
12. "3 Killed, 32 Injured in Mumbai Bomb Blast," *Times of India*, December 2, 2002, <http://timesofindia.indiatimes.com/articleshow/30087211.cms>.
13. Tarun (India), "Major Islamic Terror Attacks in India: India Is Being Attacked by Islamists from Inside as Well as Outside," Daniel Pipes (blog), October 8, 2006, <http://www.danielpipes.org/comments/59319/>.
14. Vijay Singh, "Blast Near Vile Parle Station in Mumbai, One Killed, 25 Injured," *Rediff India Abroad*, January 28, 2003, <http://www.rediff.com/news/2003/jan/27mum2.htm>.
15. Vijay Singh, "Blast in Mumbai Train, 10 Killed," *Rediff India Abroad*, March 14, 2003, <http://www.rediff.com/news/2003/mar/13mum.htm>.
16. "Parcel Bomb Kills Bandra Security Guard," *Times of India*, April 15, 2003, <http://timesofindia.indiatimes.com/articleshow/43402607.cms>.
17. Vijay Singh and Syed Firdaus Ashraf, "Blast in Ghatkopar in Mumbai, 4 Killed and 32 Injured," *Rediff India Abroad*, updated July 29, 2003, <http://www.rediff.com/news/2003/jul/28blast.htm>.
18. "A Chronology of the 2003 Mumbai Twin Blasts Case," *Rediff India Abroad*, July 27, 2007, <http://news.rediff.com/report/2009/jul/27/a-chronology-of-the-2003-mumbai-twin-blasts-case.htm>.
19. Tarun, "Major Islamic Terror Attacks in India"; "Bombay Blasts Revenge for Gujarat Riots—Indian State," *China Daily*, August 27, 2003, http://www.chinadaily.com.cn/en/doc/2003-08/27/content_258711.htm.
20. "At Least 174 Killed in Indian Train Blasts," CNN, July 11, 2006, <http://www.cnn.com/2006/WORLD/asiapcf/07/11/mumbai.blasts/index.html>.
21. "Small, Logical Steps Cracked Case: Roy," *Times of India*, October 2, 2006, <http://timesofindia.indiatimes.com/articleshow/2062187.cms>; "India Police: Pakistan Spy Agency behind Mumbai Bombings," CNN, October 1, 2006, <http://www.cnn.com/2006/WORLD/asiapcf/09/30/india.bombs/index.html>.
22. "India Police."
23. "Major Attacks and Blasts in India since 2001," Reuters, August 25, 2007, <http://in.reuters.com/article/topNews/idINIndia-29149720070825/>; "Major Attacks since 2003," *Times of India*, November 27, 2008, http://timesofindia.indiatimes.com/India/India_a_major_terror_target/articleshow/3761676.cms (site discontinued); "India: A Major Terror Target," *Hindustan Times* (New Delhi, India), September 13, 2008, <http://www.hindustantimes.com/storypage/storypage.aspx?sectionName=&id=e0a7ae2d-e33c-4eac-b5e8-41d2b78df73a&&Headline=Major+attacks+since+2003> (site discontinued).
24. "Fidayeen Storm J&K House, Kill 29," *Tribune* (Chandigarh, India), October 2, 2001, <http://www.tribuneindia.com/2001/20011002/main1.htm>; "India: A Major Terror Target," *Hindustan Times* (New Delhi, India), September 13, 2008, <http://www.hindustantimes.com/storypage/storypage.aspx?sectionName=&id=e0a7ae2d-e33c-4eac-b5e8-41d2b78df73a&&Headline=Major+attacks+since+2003> (site discontinued).
25. "Terrorists Attack Parliament; Five Intruders, Six Cops Killed," *Rediff India Abroad*, December 13, 2001, <http://www.rediff.com/news/2001/dec/13par11.htm>.
26. Kanchana Suggu, "The Militants Had the Home Ministry and Special Parliament Label," *Rediff India Abroad*, December 13, 2001, <http://www.rediff.com/news/2001/dec/13par114.htm>.
27. US Department of State, "Terrorist Organizations," chap. 6 in *Country Reports on Terrorism 2008*, April 30, 2009, <http://www.state.gov/s/ct/rls/crt/2008/122449.htm>; Anjali Mody, "4 Accused in Parliament Attack Case Convicted," *Hindu* (Chennai, India), December 17, 2002, <http://www.hinduonnet.com/2002/12/17/stories/2002121705260100.htm>.

28. Amy Waldman, "Gunmen Raid Hindu Temple Complex in India, Killing 29," *New York Times*, September 25, 2002, <http://www.nytimes.com/2002/09/25/world/gunmen-raid-hindu-temple-complex-in-india-killing-29.html>; CNN-IBN, "Akshardham Attack Verdict Today," *IBN Live*, July 1, 2006, <http://ibnlive.in.com/news/akshardham-attack-verdict-today/14271-3.html>.
29. Mukhtar Ahmad, "33 Killed in Attack on Army Camp in Jammu," *Rediff India Abroad*, May 14, 2002, <http://www.rediff.com/news/2002/may/14jk.htm>.
30. "Pakistan Army Masterminded Jammu Attack," *Rediff India Abroad*, May 16, 2002, <http://www.rediff.com/news/2002/may/16jk3.htm>.
31. Wasbir Hussain, "A Deathly Reminder," *Outlook India*, August 16, 2004, <http://outlookindia.com/article.aspx?224789>.
32. "Incidents Involving United Liberation Front of Asom (ULFA): 2010–2011," *South Asia Terrorism Portal*, updated June 19, 2011, http://www.satp.org/satporgtp/countries/india/states/assam/terrorist_outfits/ULFA_tl.htm.
33. "United Liberation Front of Asom (ULFA)—Terrorist Group of Assam," *South Asia Terrorism Portal*, http://www.satp.org/satporgtp/countries/india/states/assam/terrorist_outfits/Ulfa.htm.
34. "Blasts in New Delhi Kill 55," *CNN*, October 30, 2005, <http://www.cnn.com/2005/WORLD/asiapcf/10/29/india.explosion/index.html>.
35. "55 Killed in Three Bombs in Delhi," *Rediff India Abroad*, October 29, 2005, <http://www.rediff.com/news/2005/oct/29delhi.htm>.
36. "Police Say Bombs Work of Single Outfit," *Rediff India Abroad*, October 30, 2005, <http://www.rediff.com/news/2005/oct/30dblast3.htm>.
37. "Serial Bombs in Varanasi," *Telegraph* (Calcutta, India), March 8, 2006, http://www.telegraphindia.com/1060308/asp/frontpage/story_5941755.asp.
38. "Bombs Kill 37 in India Graveyard," *BBC News*, September 8, 2006, http://news.bbc.co.uk/2/hi/south_asia/5326730.stm.
39. "Police Arrest Malegaon Bombs 'Conspirator,'" *Times of India*, November 6, 2006, <http://timesofindia.indiatimes.com/articleshow/334758.cms>.
40. "Indian, Pakistani Leaders Pledge to Continue Talks Despite Deadly Train Bombing," *PBS NewsHour*, February 19, 2007, http://www.pbs.org/newshour/updates/asia/jan-june07/train_02-19.html.
41. "Bomb Hits Historic India Mosque," *BBC News*, May 18, 2007, http://news.bbc.co.uk/2/hi/south_asia/6668695.stm.
42. Syed Amin Jafri, "9 Killed in Hyderabad Blast; 5 in Police Firing," *Rediff India Abroad*, updated May 19, 2007, <http://www.rediff.com/news/2007/may/18blast.htm>.
43. "Death Toll in Hyderabad Serial Bombs Rises to 44," *IBN Live*, updated August 26, 2007, <http://ibnlive.in.com/news/death-toll-in-hyderabad-serial-bombs-rises-to-41/47450-3.html>.
44. "19 Bombs Found after Fatal Bombs in India," *New York Times*, August 26, 2007, <http://www.nytimes.com/2007/08/26/world/asia/26iht-india.4.7259786.html>.
45. Department of State, *Country Reports on Terrorism 2007* (Washington, DC: Department of State, 2008), <http://www.state.gov/s/ct/rls/crt/2007/>.
46. Abhishek Sharan, "HuJI, SIMI Stamp on Attacks," *Hindustan Times* (New Delhi, India), May 14, 2008, <http://www.hindustantimes.com/News/india/HuJI-SIMI-stamp-on-attacks/310684/Article1-310633.aspx>; Neha Singh, "Eight Small Bombs Hit Bangalore," *Reuters*, July 25, 2008, <http://uk.reuters.com/article/idUKISL16912820080725>; "SIMI, LeT May Be Behind Bangalore Bombs: IB," *Times of India*, July 25, 2008, http://timesofindia.indiatimes.com/SIMI_LeT_may_be_behind_Bangalore_bombs_IB_/articleshow/3279993.cms.
47. "Ahmedabad Bombs Carried Out on the Direction of Pak's Amir Raza Khan," *Times of India*, November 20, 2008, http://timesofindia.indiatimes.com/India/Ahmedabad_bombs_carried_out_on_the_direction_of_Paks_Amir_Raza_Khan/articleshow.
48. "There Will Be More Bomb Attacks, Warns Indian Mujahideen," *Economic Times* (India), September 14, 2008, <http://economictimes.indiatimes.com/articleshow/3480529.cms>.
49. Gethin Chamberlain, "Boy Killed in Terrorist Bomb Attack in Delhi," *Guardian* (London), September 28, 2008, <http://www.guardian.co.uk/world/2008/sep/28/india/>. (Initially published in the *Observer*.)
50. "3 Blown Dead: This Terror Run Isn't Over Yet," *Hindustan Times* (New Delhi, India), September 29, 2008, <http://www.hindustantimes.com/This-terror-run-isn-t-over-yet/H1-Article1-341363.aspx>.
51. Associated Press, "Explosion Kills 1, Wounds 15 in Western India," *MSNBC*, September 29, 2008, <http://www.msnbc.msn.com/id/26946171/>.
52. Mateen Hafeez and Yogesh Naik, "Bombs in Maharashtra, Gujarat; 8 Killed," *Times of India*, September 30, 2008, http://timesofindia.indiatimes.com/Bombs_in_Maharashtra_Gujarat_8_killed/articleshow/3542011.cms.
53. "Explosion in Kanpur, Seven Injured," *Indian Express*, October 14, 2008, <http://www.indianexpress.com/news/explosion-in-kanpur-seven-injured/373293/>.
54. "Imphal Blast Near Police Hub Kills 17," *Telegraph* (Calcutta, India), October 21, 2008, http://www.telegraphindia.com/1081022/jsp/nation/story_10002920.jsp.
55. "India Wants to Seal Border with Myanmar after Blast," *Reuters*, October 22, 2008, <http://www.reuters.com/article/latestCrisis/idUSDEL42232/>.

56. Biswajyoti Das, "India Suspects Islamists, Separatists in Assam Attack," Reuters, October 31, 2008, <http://www.reuters.com/article/newsOne/idUSTRE49U20V20081031/>.
57. "One Arrested for Assam Serial Blasts," *Times of India*, October 31, 2008, http://timesofindia.indiatimes.com/Assam_blasts_toll_rises_to_77_curfew_in_Ganeshguri/articleshow/3658239.cms.
58. Padma Rao Sundarji, "India's Lack of Preparedness Raised Mumbai's Death Toll," McClatchy Newspapers, December 3, 2008, <http://www.mcclatchydc.com/2008/12/03/57012/indias-lack-of-preparedness-raised.html>.
59. Steven Aftergood, "India Intelligence and Security Agencies: Intelligence Bureau," Federation of American Scientists, updated December 2006, <http://www.fas.org/irp/world/india/ib/index.html>.
60. "Why Politicians Won't Get Off the Line," *Hindustan Times* (New Delhi, India), April 24, 2010, <http://www.hindustantimes.com/Why-politicians-won-t-get-off-the-line/Article1-535365.aspx>.
61. Border Security Force, "History," <http://bsf.gov.in/Pages/History.aspx>.
62. Sundarji, "India's Lack of Preparedness."
63. Mumbai Police, "Anti Terrorism Squad," http://www.mumbaipolice.org/special/anit_terror_squad.htm.
64. Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, 2nd ed. (Washington, DC: CQ Press, 2015), 209.
65. Ibid., 144.
66. For a full explanation of Analysis of Competing Hypotheses, see *ibid.*, 181.

15 Iranian Meddling in Bahrain

By Flannery O. Becker and Sarah Miller Beebe

Key Questions

- ▶ Are Bahraini accusations about Iranian meddling true?
- ▶ Are the Iranian and opposition counteraccusations true?
- ▶ How could Iran seek to influence Bahrain?

CASE NARRATIVE

Accusations and Counteraccusations

In April 2011, Bahrain took the extraordinary step of sending a confidential report to UN Secretary General Ban Ki-moon accusing Iran of using Hezbollah to support and possibly finance the Bahrain opposition's "Arab Spring" uprising.¹ The report said that "evidence confirms that Bahraini elements are being trained in Hezbollah camps specifically established to train assets from the Gulf," in a plot to overthrow the Khalifa monarchy.² Iranian Foreign Minister Ali Akbar Salehi firmly denied the accusations, saying, "I would like to categorically reject the desperate attempts by the Bahraini authorities, who seek to implicate my government with a situation, which is only the result of their own miscalculations and missteps."³ Meanwhile, the spokesperson for al-Wefaq—Bahrain's main opposition party—issued counteraccusations, later saying, "It is easy for the regime here to utilize this conflict and blame Iran for everything happening here in Bahrain."⁴ He further noted that the regime was painting a picture of its suppression of the majority Shia opposition that would be palatable to the United States, an important ally whose Naval Fifth Fleet is stationed in Manama.⁵

Accusations of Iranian meddling are frequent and rooted in the region's long-standing power struggle between Iran and its Arab neighbors. Civil unrest has long plagued Bahrain and its ruling Sunni Khalifa family, who govern a nation in which Shias comprise nearly 70 percent of the population and are widely regarded to be victims of economic and political inequality.⁶ The Bahraini government over the past several decades has repeatedly cited foreign influence when taking steps to suppress internal opposition movements and jail resistance figures. By taking the unprecedented step of appealing to the United Nations, however, Bahrain took its accusations to a new level.

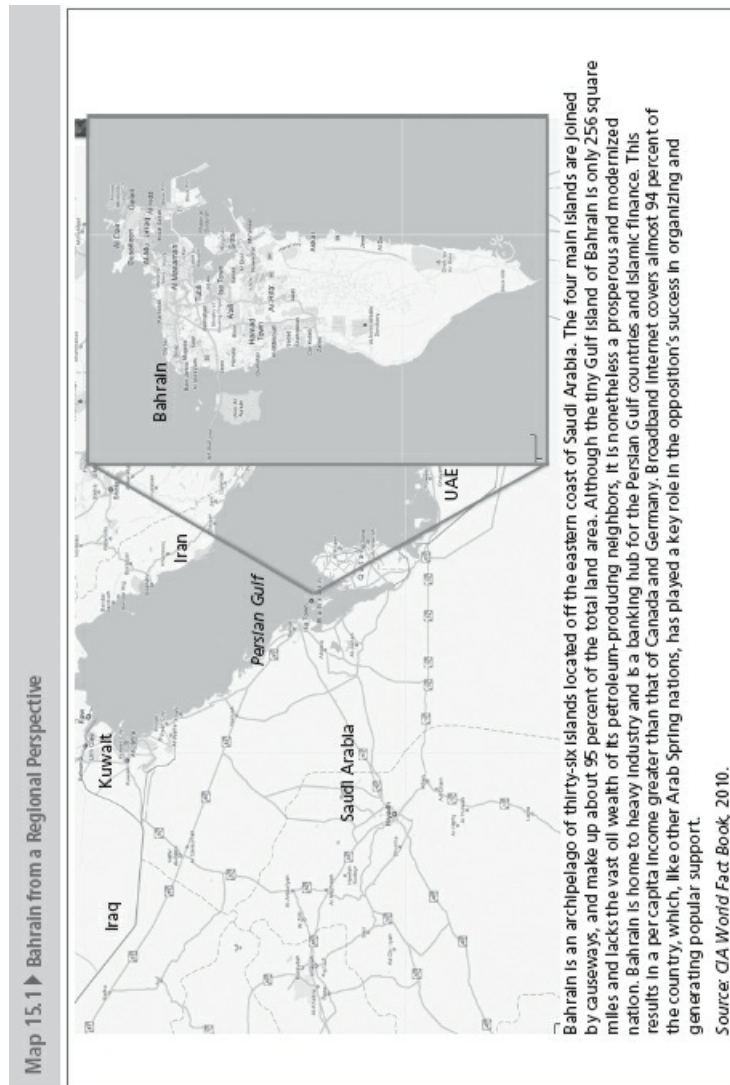
In the face of these conflicting claims and counterclaims, observers and analysts were left to

navigate the sea of facts and allegations about Iranian meddling. The ramifications for the United States were significant: if Bahraini government claims were true, US policy had to address the prospect of a proxy war between Iran and Saudi Arabia, Bahrain's Sunni neighbor to the West; if opposition counterclaims and Iranian denials were true, US policy would more naturally focus on the question of how domestic reforms might address opposition grievances.

Sunni Power, Shia People

Prior to its incarnation as a Sunni monarchy, Bahrain was intermittently part of the vast Persian Empire for more than a millennium. Various Arab tribes inhabited the small island, measuring roughly one-fifth the size of Rhode Island, until it was formally annexed by the Persian Empire in the fourth century AD. It was not until 1783 that the Khalifa family, who arrived from a central Arabian tribe, expelled the Persians and laid claim to the sheikhdom of Bahrain.⁷ In 1868, as European colonialism expanded in Africa and the Middle East, Bahrain became part of the British-Trucial states. Additional treaties entered into by the Khalifas in 1880 and 1892 granted Britain authority over British and foreign nationals living in Bahrain and forbade Bahrain from entering into hostilities with other nations without prior British consent.⁸ As its foothold in Bahrain grew, Britain moved its military base from Aden, Yemen, to Manama, Bahrain, in 1966, where it remained until 1971, a year after Bahrain finally gained its independence.⁹ Although Britain withdrew its military presence from the island, it left behind a large and functional military base. (See Map 15.1.)

Iran had formally lost control over Bahrain in the eighteenth century, but it continued to exert its claim to the former province for several centuries. As of 1970, Iran and Britain were in disagreement about the future status of Bahrain. Britain considered the island a sovereign Arab state. Iran never acknowledged the legitimacy of the British protectorate but instead viewed Bahrain as the fourteenth Persian province, stating that “the protection which Britain has asserted for more than a century over these Islands has prevented Iran from exercising her legitimate rights there.”¹⁰ In March 1970, the Iranian representative to the United Nations sent a letter to the secretary general requesting the Security Council to ascertain the “true wishes of the people of Bahrain” in regard to their future status.¹¹ The subsequent report found that an overwhelming majority of the Bahraini people preferred independence, finally forcing Iran to relinquish its long-standing claim over the island.¹²



Fear of Persian hegemony did not abate in Bahrain following Iran's concession to the United Nations, however. Bahrain adopted a constitution and elected its first parliament in 1973, but in August 1975 the emir disbanded the National Assembly in response to its effort to end Al-Khalifa rule and expel the US Navy from Bahrain. Following the 1979 Iranian Revolution, Bahrain's concern for its independence from Iranian control was grounded less in Iran's military and political power than in the spread of Shia religious influence flowing from the new Islamic theocracy. The Khalifa family and other Gulf State Sunni monarchs ruling over large Shia populations realized that an Iranian-backed Shia uprising might pose the most potent threat yet to their fragile monarchies.

In 1981, the Khalifa family's fears came to fruition when the government broke up what it regarded as a *coup d'état* led by the Islamic Front for the Liberation of Bahrain (IFLB), a local Shia resistance group formed in 1975 and supported financially and logistically by the newly powerful Iranian clerical regime.¹³ The IFLB, which was headquartered in Tehran but comprised solely of Bahrainis, closely and openly supported the Iranian Islamic Republic and even sent members to fight in the Iran–Iraq War.¹⁴ As a Shia opposition movement from its inception, the IFLB had strongly supported the Ayatollah Khomeini's rise to power and the establishment of

the Islamic Republic in 1979. The IFLB publicly declared its support, saying, “Victory to the Islamic world revolution under Imam Khomeini! Long live the struggle of our faithful Bahraini people!”¹⁵ After uncovering the attempted coup in 1981, the Khalifa government summarily arrested three hundred IFLB supporters and tried seventy-three who were suspected of complicity.¹⁶ Many IFLB members and leaders who had evaded the first round of arrests fled the country and formed new Bahraini resistance leagues in Lebanon, the United Kingdom, and Iran. Although the IFLB formally dissolved in the late 1990s, many members returned to Bahrain in 2001 to once again organize and lead oppositionist activities.

The 1981 attempted coup caused great concern among Gulf leaders who were beginning to appreciate that religion could be a more powerful agent of change than nationalism. Although the status of Shias in Bahrain was a chronic concern, few had expected such a radicalized rebellion among a native population that was economically stable. Although the IFLB represented a tiny fraction of the Bahraini Shias at the time, the rise of transnational Shiism represented by the IFLB galvanized other Shia subpopulations in the early 1980s to organize and demand change. Whether those opposition ties to Iran remained latent within the Shia population or dissipated over the ensuing thirty years remains unclear.

Bahraini Shias and Iranian Shias: Religious Similarities, Ethnic Differences

The 1979 Islamic Revolution had a profound effect upon the Shia populations throughout the Middle East and in Islamic communities around the world. Shias were proud of the new Islamic theocracy, especially those living under Sunni dominance or secularism. This sympathetic feeling toward the Islamic Republic, however, did not necessarily stem from a desire for similar political change in their home countries, but rather arose from a respect for Iran as a powerful Shi’ite influence in the region.¹⁷ The Bahraini Shias in particular were emboldened by their powerful Shia neighbor, but they still regarded themselves as distinctive Bahraini Shias and not Iranian Shia proxies (see Table 15.1).

Linguistic and ethnic differences clearly distinguished the Arab Bahraini Shia from their Persian neighbors. The Bahrainis are Arabs from the Baharna tribe and speak Arabic. The Iranians, by contrast, are of Persian decent and speak Farsi. These distinctions are highly significant to Bahraini national identity and, to some, transcend the important but secondary religious affinity with Iranian Shias.

Table 15.1 ▶ Distinctions between Bahraini and Iranian Shias		
	Bahraini Shia	Iranian Shia
Tribe	Bahama	Persian
Language	Arabic	Farsi
Religious Doctrine	Akhbari	Usuli

Source: Laurence Louër, *Transnational Shia Politics: Religious and Political Networks in the Gulf* (New York: Columbia University Press, 2008), 111.

Fundamental divergences in Shi’ite legal thought between the two nations further mitigated strong cross-national religious ties. Whereas Iran and a vast majority of the Shia world follow the

Usuli doctrine of Islamic law, Bahrain remains one of the only places in the world where Akhbari scholarship is strongly maintained. The Akhbaris are considered “quietists” by nature, believing that clerics should have only an advisory role in society and should not be political leaders. This doctrine markedly contrasts with that of Iranians, who justify the political and religious guidance of the Supreme Leader through the Usuli doctrine.¹⁸ Although it is debatable whether some influential Shia clerics in Bahrain continue to follow strict Akhbari doctrine, many remain fiercely loyal to the school’s main principles.¹⁹

Bahrain’s Sunni and Shi’ite Citizens: More Than Religious Differences

Although they are joined under a common nationality, there is a chasm between Bahraini Shias and Bahraini Sunnis, who are set apart not only by ancient religious divisions but also by social, economic, and linguistic differences. In many respects, it is these boundaries that are potentially more divisive to Bahraini national unity than Islamic sectarianism.

Bahrain has enjoyed enormous economic growth over the past twenty years, although it is generally perceived that the majority of Shias do not share equitably in this wealth. Accurate estimates are difficult to obtain, but one recent measure shows that income inequality remains high, and relative poverty is estimated to be between 30 and 40 percent.²⁰ Shias are routinely barred from government employment, especially in the security forces, and many complain that private sector jobs are given to foreign workers who will accept lower wages. Moreover, although Shias comprise a majority of the Bahraini national population, they represent only a small number of elected officials. The Khalifa regime has been accused of electoral gerrymandering to allow sparsely populated Sunni areas to be overrepresented in the legislature. In the opinion of some critics, the resulting political imbalance reinforces sectarian division through disenfranchisement of an otherwise majority population.

Adding to the bitter taste of inequality and separation, the Shias and Sunnis of Bahrain traditionally speak in different dialects of colloquial Arabic. Because Saudi Arabia’s Eastern Province and present-day Bahrain were once united, Arab Shias in both countries speak the same form of Arabic dialect, whereas the Sunnis typically use a Bedouin dialect that is shared among other Sunni Gulf populations.²¹

Instability in the 1990s

Following a period of political stasis, social marginalization, and rising unemployment, young Bahraini Shias took to the streets in late 1994 to protest worsening economic conditions. The *intifada*, which lasted until 1999, began as a spontaneous revolt among the country’s youth. It later gained traction and greater attention when it caught the attention of international Bahraini organizations and human rights nongovernmental organizations (NGOs). The Islamic Bahrain Freedom Movement (IBFM) (*Harakat Ahrar al-Bahrain al-Islamiyya*), led by London-based Bahraini expatriate Saeed Shihabi, drew attention to the movement. Shihabi himself had allegedly been involved in the earlier turmoil of the 1980s in Bahrain.²² This time, the IBFM downplayed the uprising’s Islamic roots and characterized it as a popular democratic movement, a move that Shihabi hoped would gain sympathy with a Western audience. Shihabi, along with other Bahrainis living in the United Kingdom, lobbied Amnesty International, the United Nations, and even members of the British Parliament to intervene on their behalf in the situation.

The UK-based IBFM also maintained close contact with the movement’s leaders on the

ground. A young cleric named Ali Salman emerged as a leading figure of the *intifada*, although he appeared to have had no previous political involvement. Bahraini authorities forced Salman to leave the country in 1995 for participating in the protests, but instead of heading to Lebanon or Qom (where he had conducted his religious studies), Salman went to London, where he became involved with the IBFM.

Supporting the opposition movement from abroad was Sheikh Muhammad Ali al-Mahfouz, the secretary general of the then-exiled IFLB. Mahfouz conveyed his messages of solidarity to the movement from an apartment outside of Beirut, where he had sought refuge after fleeing Bahrain with other IFLB members in the early 1980s.²³ Although Mahfouz remained exiled from Bahrain, he, as well as other expatriated influential Bahrainis, eventually returned to his home country as a celebrated hero among the local Shias.

The uprisings of the mid-1990s highlighted the growing tensions on the tiny island, which were not solely sectarian in nature but had a variety of root causes. The protests often embraced both Shias and Sunnis who were united in calling for greater political reform. Together they petitioned the monarchy for changes in socioeconomic policy and called for a return to constitutional democracy.²⁴ The Bahraini people had been governed under emergency law since the Al-Khalifa emir abrogated the constitution in 1975, just two years after it had been adopted.

The *intifada* lasted from 1994 to 1999 and was marked by violence on all sides, leaving dozens dead and hundreds injured, a significant number for a country of only 600,000 people. Government security forces imprisoned the leaders of the opposition movement and allegedly used brute force to suppress the street protests.²⁵ Several small dissident groups launched a series of retaliatory bombings on government buildings, luxury hotels, and local businesses—actions that served only to further aggravate and divide the already fractured society. A man who claimed to speak for the IFLB initially proclaimed culpability for an explosion at the Diplomat Hotel in February 1996, although the group later denied any connection to the bombing.²⁶

During these years of political turbulence, Bahrain agreed to forge a stronger relationship with the West by signing an agreement with the United States allowing use of the former British naval base in Manama. In 1995, the United States reactivated its Fifth Naval Fleet, which is responsible for large-scale operations in the Persian Gulf, Red Sea, and Arabian Sea.

The Khalifas' delicate relationship with the West has recently been complicated by Saudi Arabia's influence in the Gulf nation. Involvement in Bahraini politics is nothing new to the Saudis. In addition to providing Bahrain with oil subsidies, the Saudi regime maintains close ties with the Khalifa family.²⁷ The Saudi monarchy seeks to minimize Iran's influence in the region and has long feared that a popular uprising in Bahrain could lead to instability in Saudi Arabia's nearby Eastern Province, which contains the nation's largest oil and gas reserves and is home to a large Shia population. (See Table 15.2.) In a move that revealed his concerns, the Saudi king granted Saudi citizens, including the Eastern Province Shias, more than \$10.7 billion in benefits on 23 February, shortly after the Arab Spring emerged in Bahrain.²⁸

Reforms Bring Only Temporary Relief

The instability of the 1990s abated momentarily after the Khalifa emir died in 1999 and his son Shaikh Hamad bin Isa Al Khalifa ascended to power. In an effort to mend relations with the nation's Shias and usher in some semblance of stability and peace, Hamad announced a series of political and social reforms, the linchpin of which was his intention to reinstate a constitutional monarchy, which proffered him the title of king. He also proposed extending full voting rights to

women and opening the political arena to opposition parties.³⁶ Hamad's 2001 referendum was approved by 98 percent of voters, who participated in record numbers and gave the new king a popular legitimacy that the Khalifas had never before enjoyed.³⁷ Further relieving internal tensions, Hamad announced that municipal and legislative elections would be held in 2002 and that all political prisoners and exiled Bahraini citizens would be granted a general pardon.

Table 15.2 ▶ Examples of Iranian Influence in the Middle East

Country	Examples of Iranian Influence
Afghanistan	In the 1990s, Iran waged a proxy war against the Taliban and other Islamic extremists via financial and material support to the Northern Alliance. ²⁹ In post-Taliban Afghanistan, Iranian influence has at times been more direct; in 2010, President Hamid Karzai admitted that his chief of staff received bags of money from Iran that Karzai later said were ostensibly meant as aid. ³⁰ By 2012, Western media reported that Tehran was undertaking a multifaceted influence operation in Afghanistan that involved "cultivating closer relations with the Taliban, funding politicians and media outlets, and expanding cultural ties with its eastern neighbor." ³¹
Iraq	After a long war with Iraq in the 1980s that reverberated throughout the 1990s, Iran's primary objective today is to use its influence to prevent Iraq from recovering as a military threat. Tehran has used a range of tools to do so, including backing militancy inside Iraq, fostering economic codependence, and integrating eastern Iraq's energy infrastructure into its own, in addition to "providing campaign financing, media support . . . and paramilitary support to armed groups" that are aligned with Iranian interests. ³²
Lebanon	Iran helped to establish Hezbollah in the early 1980s, and has since used the Shia opposition group to exert influence in Lebanon and deter Israel. In more recent years, however, their ties have evolved from that of a proxy relationship to a partnership as Iran and Hezbollah work to deter Israel and the West. ³³ Iran has used its Iranian Revolutionary Guard Corp to "teach Hezbollah how to organize itself like an army, with special units for intelligence, antitank warfare, explosives, engineering, communications and rocket launching." ³⁴
Syria	Iran has had a long and close relationship with Syria, which it has used as a pipeline to funnel weapons and other support to Hezbollah and Hamas. In the wake of demonstrations across Syria in 2011 and 2012, Iran allegedly provided Syria with equipment used to "disperse the country's prodemocracy protests and is helping Syrian security forces block and track Internet and cell phone use among protesters." ³⁵

After this formal declaration of amnesty, many former opposition leaders of the 1990s *intifada* returned from abroad to once again nurture Shia opposition parties. Perhaps one of the most notable examples of this is Ali Salman, the exiled cleric who had directed many popular protests in 1994. Upon his return, he established and became the head of Bahrain's largest and most influential opposition party, al-Wefaq.

The king's broad popularity was short lived. In 2002, Hamad proclaimed Bahrain a constitutional monarchy and changed his title from emir to king. Although al-Wefaq initially supported the king's 2001 referendum, it withdrew its support from his 2002 constitution, which it viewed as extending and concentrating the monarch's authority.

The constitution established a bicameral parliament that consists of a forty-member elected Council of Representatives and a forty-member Shura (Consultative) Council appointed by the

king. Members of both chambers serve four-year terms. With direct control over appointments to one chamber, Hamad effectively possessed veto power over any legislation.³⁸ Additionally, the electoral constituency map was apportioned in such a way as to limit the number of representatives that Bahraini Shia could gain in the Chamber of Deputies. Thus, heavily populated Shia areas received the same number of representatives as sparsely populated Sunni neighborhoods.

Further adding to Shia disillusionment, the government naturalized hundreds of Sunni expatriates and, contrary to the practices of other Sunni monarchies in the region, granted them the right to vote. For all of these reasons, al-Wefaq and three other opposition political parties decided to boycott legislative elections in October 2002.³⁹



King Hamad bin Isa Al Khalifa proclaimed Bahrain a constitutional monarchy in 2002 and changed his title from emir to king.

Renewed tensions between the Shias and the monarchy marred the political scene as democratic reforms advanced at a glacial pace. The Khalifas systematically blocked the opposition's attempts to galvanize support for the abrogation of the 2002 constitution in favor of the more liberal 1973 constitution. In an effort to quell dissenting voices, King Hamad shut down opposition print media, arrested and jailed human rights leaders, restricted the activities of political organizations, and monitored the Twitter and Facebook accounts of opposition groups.⁴⁰

Day of Rage: The Arab Spring Takes Root

In early 2011, as the Arab Spring gained footholds in Tunisia and Egypt, Shia Bahrainis used Twitter and Facebook to organize their own demonstration for 14 February, the tenth anniversary of the 2001 referendum that had promised greater democratic change. The government's reaction to the demonstration was initially muted. At the outset, protesters complained only about slow Internet connections, raising questions about whether the government had forced service providers to reduce speeds in order to slow the dissemination of information.⁴¹

What began as peaceful pro-reform sit-ins and gatherings at the symbolic Pearl Roundabout in Manama escalated suddenly and violently overnight on 17 February when Bahraini Defense

Forces raided the makeshift camp and opened fire on sleeping protestors.⁴² Dozens of protestors were rushed to the emergency rooms, six people died as a result of their injuries, and many suffered serious wounds.⁴³ The raid emboldened demonstrators who took to the streets in even greater numbers. The tone of the protests changed after the assault: initial calls for mild political reforms to reduce perceived discrimination against Shia Bahrainis were replaced with direct challenges to the monarchy itself.⁴⁴ The political crisis only deepened when al-Wefaq parliament member Abdul-Jalil Khalil announced that the party would withdraw from the parliament, where it held eighteen out of forty seats, citing “aggressive attacks by the police on civilians demonstrating and carrying the kingdom’s flag and calling for political and constitutional reforms.”⁴⁵



Pearl Roundabout before and after the 14–17 February protests. Protesters gather on 14 February 2011 at Pearl Roundabout in Manama (left); police survey the scene after dispersing protesters on 17 February 2011 (right).

By March, with the protests exhausting the resources of the Khalifa monarchy, Bahrain requested help. Under the auspices of the Gulf Cooperation Council (GCC), Saudi Arabia and other GCC states sent one thousand troops across the sixteen-mile King Fahd Causeway to Bahrain on 14 March. The troops’ official mandate was “to protect vital facilities, such as oil, electricity and water installations, and financial and banking facilities.”⁴⁶ The ensuing violence claimed even more lives as Bahrain instituted a state of emergency and instructed GCC troops to “to take all measures to quell a festering rebellion.”⁴⁷ In the wake of renewed violence, the opposition’s public statements only muddled the water and fueled speculation about its ties to Iran. In an interview with *Al Akhbar* newspaper, opposition leader Hassan Mushaima of the al-Haq party said that if Bahraini leaders allowed Saudi Arabia to intervene militarily, then the opposition had the right to appeal to Iran for support.⁴⁸ In response to the deployment, Iran’s Foreign Minister, Ali Akhbar, urged Gulf States who sent troops to the kingdom to act with “wisdom and caution.”⁴⁹ Bahrain immediately recalled its ambassador to Tehran. Tensions between Iran and Saudi Arabia also intensified as each country accused the other of using Bahrain to pursue its own agenda.⁵⁰

In the midst of rising violence, the sides searched for a solution. King Hamad met with the leaders of al-Wefaq and promised national dialogue, enhanced powers for the parliament, electoral reform, and a nationwide referendum on any new changes.⁵¹ However, the hope of reconciliation paled as GCC and Bahraini troops enforced martial law and made prominent arrests. On 17 March, the government arrested eight opposition members whom it accused of running a “sedition ring” that called “for the downfall of the regime” and had “intelligence

contacts with foreign countries.”⁵² (See Table 15.3.) Opposition members denied the claims. By April 2011, the government took the extraordinary step of appealing to the UN secretary general. Were the accusations true, or were they merely another effort to discredit the opposition?

Table 15.3 ► Bahraini Opposition Members Arrested on 17 March 2011

Name	Affiliation and Background
Ibrahim Sharif	Secretary general of the Wa’ad National Democratic Action Society, a secularist political opposition association. Formed a loose coalition with al-Haq and al-Wefaq to demand democratic reforms. Wa’ad has called for transformation to true constitutional democracy.
Hassan Mushaima	Leader of the al-Haq Movement of Liberties and Democracy, a Shia opposition group. He lived in exile in the United Kingdom until February 2011, when he returned to Bahrain following a general amnesty issued by King Hamad. Formed a loose coalition with Wa’ad and al-Wefaq to demand democratic reforms.
Abdul-Wahab Hussein	President of the al-Wefaq Islamic Movement. Formed a loose coalition with Wa’ad and al-Haq to demand democratic reforms. Joined with al-Haq in the Coalition for a Republic to call for abolition of the monarchy.
Abdul-Jalil al-Singace	Leading member of the al-Haq Movement, a Shia opposition group. He was previously detained from August 2010 until the February 2011 general amnesty. Joined with al-Wefaq in the Coalition for a Republic to call for abolition of the monarchy.
Shaikh Saeed al-Nuri	Cleric and political activist. He was previously detained from August 2010 until the February 2011 general amnesty.
Shaikh Abd al-Hadi al-Mukhodher	Cleric and political activist. He was previously detained from August 2010 until the February 2011 general amnesty. Generally viewed as being aligned with those seeking radical changes in the power structure.
Hassan al-Haddad	Member of the Committee of the Unemployed. He was previously detained from August 2010 until the February 2011 general amnesty. Generally viewed as being aligned with those seeking radical changes in the power structure.
Ali al-’Ekri	A medical doctor in al-Salmaniya and a protest organizer. Generally viewed as being aligned with those seeking radical changes in the power structure.

Sources: “HRW: Bahrain: Protest Leaders Arbitrarily Detained,” Human Rights Watch, March 18, 2011, <http://www.hrw.org/news/2011/03/18/bahrain-protest-leaders-arbitrarily-detained>; “Bahrain: Eight Activists Detained in Bahrain,” Amnesty International, March 18, 2011, <http://www.amnesty.org/en/library/asset/MDE11/014/2011/en/2a6208ad-6194-4311-ae9a-6762bcd87b07/mde110142011en.html>.

RECOMMENDED READINGS

Deeb, Lara. *The Enchanted Modern: Gender and Public Piety in Shi’i Lebanon*. Princeton, NJ: Princeton University Press, 2006.

Louër, Laurence. *Transnational Shia Politics: Religious and Political Networks in the Gulf*. New York: Columbia University Press, 2008.

Table 15.4 ▶ Case Snapshot: Iranian Meddling in Bahrain

Structured Analytic Technique Used	Heuer and Pherson Page Number	Analytic Family
Structured Brainstorming	p. 102	Idea Generation
Starbursting	p. 113	Idea Generation
Morphological Analysis	p. 119	Idea Generation
Indicators	p. 149	Scenarios and Indicators

IRANIAN MEDDLING IN BAHRAIN

Structured Analytic Techniques in Action

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.

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 (see Figure 15.1) 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.

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 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.

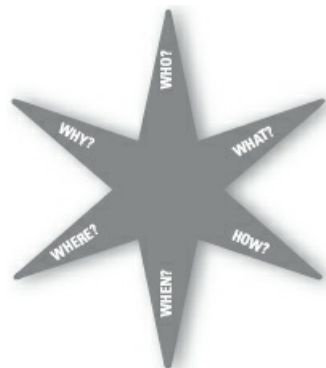
STEP 3: After generating questions that start with each of the six words, the group should either prioritize the questions to be answered or sort the questions into logical categories.

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?

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.

Figure 15.1 ▶ Starbursting Template



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.) 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.

STEP 4: Eliminate any combinations that are impossible, impractical, or undeserving of attention.

STEP 5: Refine the scenarios so that they are clear and concise.

Table 15.5 ▶ Morphological Analysis Template

Dimensions			
Group	Bahraini opposition members		
Activity	Receiving training in Iranian-backed Hezbollah camps		
Method	Clandestine		
Impact	Overthrow the Khalifa monarchy		

Analytic Value Added. Which scenarios are most deserving of attention? Do any assumptions underlie the scenarios? Are there any information gaps that affect your ability to assess the likelihood of a scenario?

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.)

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.

Box 15.1 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 discuss 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 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.
- 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.

Analytic Value Added. What affinity clusters emerged? What are the key dimensions of problem?

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.

Task 4. Using the Structured Brainstorming results to prompt your thinking, create tailored

indicators for each of main scenarios developed in Task 2: Morphological Analysis.

STEP 1: Create a list of the most attention-deserving scenarios to track for this case.

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, 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 collectable 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.

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?

NOTES

1. Jay Solomon, "Bahrain Sees Hezbollah Plot in Protest," *Wall Street Journal*, April 25, 2011, <http://online.wsj.com/article/SB10001424052748703907004576279121469543918.html>.
2. Ibid.
3. Ibid.
4. Phillip Walter, "Bahrain Opposition Fears Effects of Iran-West Tensions," *Voice of America*, January 30, 2012, <http://www.voanews.com/english/news/middle-east/Bahrain-Opinion-Fears-Effects-of-Iran-West-Tensions-138324239.html>.
5. Ibid.
6. Condoleezza Rice, *No Higher Honor: A Memoir of My Years in Washington* (New York: Random House, 2011), 369.
7. David Lea, *A Political Chronology of the Middle East* (London: Routledge, 2001), 17.
8. Lobna Ali Al-Khalifa, *Foreign Direct Investment in Bahrain* (Boca Raton, FL: Universal Publishers, 2010), 84.
9. Thomas M. Leonard, *Encyclopedia of the Developing World*, Vol. 1 (New York: Routledge/Taylor & Francis, 2006), 133.

10. United Nations Security Council Resolution 287 (1970), Secretary General Note to the Security Council S/9772, *Middle East Journal* 24, no. 3 (Summer 1970), <http://www.jstor.org/stable/4324618>, 373–80.
11. Secretary General of the United Nations, Note to the Security Council, March 28, 1970, S/9726, Good Offices of the U.N. Secretary-General with Regard to Bahrain, *International Legal Materials* 9, no. 4 (July 1970): 787–805, <http://www.jstor.org/stable/20690657>.
12. UN Security Council Meeting #1536, May 11, 1970, New York, http://search.un.org/search?q=iran+1970+Bahrain&ie=utf8&oe=utf8&output=xml_no_dtd&site=ods_un_org&filter=p&proxystylesheet=UN_ODS_test&clie
13. In a 2006 interview with a Bahraini daily newspaper, former IFLB member Murtadha Badr stated that Front members met with Imam Khomeini in France using money and false passports given to them by Iran. Laurence Louër, *Transnational Shia Politics: Religious and Political Networks in the Gulf* (New York: Columbia University Press, 2008), 178.
14. “Islamic Front for the Liberation of Bahrain Interview,” BBC, October 11, 1980, LexisNexis.
15. “Ramadan Statement by Islamic Front for the Liberation of Bahrain,” BBC, July 13, 1980, LexisNexis.
16. R. K. Ramazani, “Shi’ism in the Persian Gulf,” in Juan R. I. Cole and Nikki Keddie, eds., *Shiism and Social Protest* (New Haven, CT: Yale University Press, 1986), 49.
17. Graham E. Fuller and Rend Rahim, *The Arab Shi’a: The Forgotten Muslims* (New York: Palgrave Macmillan, 1999), 123.
18. Louër, *Transnational Shia Politics*, 19.
19. Ibid., 111.
20. Ala’a Shehabi, “From National Celebration to Day of Rage,” *Open Democracy*, February 12, 2011, <http://www.opendemocracy.net/ala-shehabi/bahrain-from-national-celebration-to-day-of-rage>.
21. Clive Holes, *Dialect, Culture and Society in Eastern Arabia*, Part 1, Vol. 51 (Leiden: Brill, 2001), XXI–XXIII.
22. Louër, *Transnational Shia Politics*, 202.
23. The Kuwaiti newspaper *Al-Siyassah* alleged that Mahfouz lived outside of Beirut in 1994 and received his orders from Tehran through Hezbollah. “Bahrain Says Riots Instigated by Foreign ‘Troublemakers,’” Associated Press, December 26, 1994, LexisNexis.
24. Yvonne Yazbeck Haddad and John Esposito, *Islam, Gender and Social Change* (Oxford: Oxford University Press, 1998), xxiv.
25. Julie Chernov Hwang, *Peaceful Islamist Mobilization in the Muslim World: What Went Right* (New York: Palgrave MacMillan, 2009).
26. Henry E. Mattox, *Chronology of World Terrorism, 1901–2001* (Jefferson, NC: McFarland, 2004), 136.
27. “Bahrain Oil Minister: Fuel Subsidies Will Continue to Soar,” *Khaleej Times*, November 22, 2010, http://menafn.com/menafn/qn_news_story_s.aspx?storyid=1093378358.
28. “Saudi King Announces New Benefits,” Al Jazeera, February 23, 2011, <http://www.aljazeera.com/news/middleeast/2011/02/2011223105328424268.html>.
29. Amir Bagherpou and Asad Farhad, “The Iranian Influence in Afghanistan,” *Frontline*, August 9, 2010, <http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/08/the-iranian-influence-in-afghanistan.html>.
30. “US ‘Concerned’ about Iran Influence in Afghanistan,” *Telegraph*, October 26, 2010, <http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/8086823/US-concerned-about-Iran-influence-in-Afghanistan.html>.
31. Ernesto Londoño, “Iran Intensifies Efforts to Influence Policy in Afghanistan,” *Washington Post*, January 4, 2012, http://www.washingtonpost.com/world/asia_pacific/iran-strives-to-play-spoiler-in-afghanistan/2012/01/01/gIAZ6gCbP_story.html.
32. Michael Knights, “Iran’s Influence in Iraq: Game, Set but Not Match to Tehran,” *Guardian*, October 17, 2010, <http://www.guardian.co.uk/world/2010/oct/17/iran-influence-iraq-tehran>.
33. Emile Hokayem, “Iran and Hezbollah: The Balance of Power Shifts in Lebanon,” PBS, January 27, 2011, <http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2011/01/iran-and-hezbollah-the-balance-of-power-shifts-in-lebanon.html#ixzz1qREJSAGt>.
34. “Hezbollah,” *New York Times*, December 11, 2011, <http://topics.nytimes.com/top/reference/timestopics/organizations/h/hezbollah/index.html>.
35. Ariel Zirulnick, “US Officials: Iran Helping Syria’s Assad Put Down Protests,” *Christian Science Monitor*, April 14, 2011, <http://www.csmonitor.com/World/terrorism-security/2011/0414/US-officials-Iran-helping-Syria-s-Assad-put-down-protests>.
36. “The Report: Emerging Bahrain 2007,” Oxford Business Group, November 27, 2007, <http://www.oxfordbusinessgroup.com/product/report/report-emerging-bahrain-2007>.
37. Louër, *Transnational Shia Politics*, 238.
38. Anoushiravan Ehteshami and Steven M. Vright, *Reform in the Middle East Oil Monarchies* (New York: Garnet & Ithaca Press, 2008), 84.
39. Louër, *Transnational Shia Politics*, 239.
40. Ibid., 255.

41. Ian Black, "Bahrain Police Open Fire on Funeral Procession Leaving One Dead," *Guardian*, February 15, 2011, <http://www.guardian.co.uk/world/2011/feb/15/bahrain-police-funeral-procession>.
42. Martin Chulov, "Bahrain's Quiet Anger Turns to Rage," *Guardian*, February 17, 2011, <http://www.guardian.co.uk/world/2011/feb/17/bahrain-quiet-anger-turns-rage>.
43. "Clashes Rock Bahraini Capital," *Al Jazeera*, February 17, 2011, <http://www.aljazeera.com/news/middleeast/2011/02/201121714223324820.html>.
44. Martin Chulov and Mark Tran, "Bahrain Soldiers Fire on Protesters," *Guardian*, February 18, 2011, <http://www.guardian.co.uk/world/2011/feb/18/bahrain-soldiers-fire-on-protesters>.
45. Black, "Bahrain Police Open Fire."
46. David S. Cloud and Neela Banerjee, "Saudi Arabian, Gulf Forces Enter Bahrain," *Los Angeles Times*, March 15, 2011.
47. Martin Chulov, "Bahrain Declares Martial Law as Protesters Clash with Troops," *Guardian*, March 15, 2011, <http://www.guardian.co.uk/world/2011/mar/15/bahrain-martial-law-protesters-troops>.
48. <http://abna.ir/data.asp?lang=3&Id=229108>.
49. Ibid.
50. Ibid.
51. Simon Tisdall, "Bahrain Royal Family Welcomes Saudi Troops to Face Down Violent Protests," *Guardian*, March 14, 2011, <http://www.guardian.co.uk/world/2011/mar/14/bahrain-saudi-troops-violent-protests>.
52. "HRW: Bahrain: Protest Leaders Arbitrarily Detained," Human Rights Watch, March 18, 2011, <http://www.hrw.org/news/2011/03/18/bahrain-protest-leaders-arbitrarily-detained>.

16 Shades of Orange in Ukraine

Key Questions

- ▶ What events, issues, or other factors will shape the outcome of the Ukrainian presidential election?
- ▶ What opportunities does the United States have to influence the outcome?
- ▶ What are the implications of the election for US interests in the region?

CASE NARRATIVE

On 18 March 2004, analysts in Washington, D.C., awoke to the news that Ukrainian politics had moved in two contrasting directions. The Rada, Ukraine's parliament, voted that day to establish 31 October 2004 as the date for the country's presidential election, setting the stage for a historic transfer of power through the ballot box.¹ A few blocks away at the Constitutional Court, however, justices took an important step toward emasculating that transfer by validating President Leonid Kuchma's constitutional reform bill aimed at shifting the power to appoint Ukraine's government from the president to the legislature (see Box 16.1; Figure 16.1). Ukraine's opposition cried foul, accusing the unpopular Kuchma and his allies of scheming to retain power even if they were unable to win reelection. Presidential hopeful Viktor Yushchenko reacted to the court's ruling by announcing that his opposition bloc would use "all available means," including "taking people to the street and blocking the parliamentary rostrum," to prevent adoption of the constitutional reform bill.²

Box 16.1 KUCHMA'S PROPOSED CONSTITUTIONAL CHANGES

Constitutional reform had been a priority issue for President Leonid Kuchma since his election in 1994. He succeeded in winning approval of a new constitution in 1996—Ukraine's first since the 1978 model that governed the Ukrainian Soviet Socialist Republic—which tilted the balance of power from the legislature to the presidency, and for several years thereafter he continued to press for amendments that would further enhance presidential powers at the expense of the Rada. As Kuchma's popularity declined, however, he became intent on reversing that course, and in March 2003 he proposed a series of amendments that would transform Ukraine into what was termed a European-style "parliamentary-presidential state," with several powers transferring from the

executive to the Rada.

- ▶ The prime minister and most government ministers would be appointed by the parliament and not by the president.
- ▶ The legislature's term of office would be extended to five years, and its elections would be held simultaneously with presidential elections.
- ▶ The unicameral 450-seat Rada would be replaced by a bicameral parliament with a 300-seat lower chamber and an upper chamber consisting of three representatives from each of Ukraine's twenty-seven regions.
- ▶ All seats in the lower chamber would be elected from party lists, as opposed to half from party lists and half from single-seat constituencies.
- ▶ The president would be elected by popular ballot in October 2004, but as of 2006 would be elected by a vote in the legislature.ⁱ

These provisions were slightly modified during the course of the next year, and the version ruled constitutional by the court in March 2004 provided for the prime minister to appoint most government ministers, subject to legislative approval, and for continued popular election of the president.ⁱⁱ

i. Oleg Varfolomeyev, "Kuchma's Reform Draft: A Trap for the Opposition?" *Russia Eurasia Review* 2, no. 7 (2003), [http://www.jamestown.org/single/?no_cache=1&tx_ttnews\[tt_news\]=28407&tx_ttnews\[backPid\]=226](http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=28407&tx_ttnews[backPid]=226).

ii. Jan Maksymiuk, "Ukraine Faces Radical Changes in Its Constitutional System," *Ukraine Weekly*, January 11, 2004, <http://www.ukrweekly.com/old/archive/2004/020404.shtml>.

Figure 16.1 ▶ The Rada and the Constitutional Court Split, 18 March 2004



The Rada, Ukraine's parliament, votes to establish 31 October 2004 as the date for the country's presidential election, setting the stage for a historic transfer of power through the ballot box. Meanwhile, the Constitutional Court takes an important step toward emasculating that transfer by approving President Leonid Kuchma's constitutional reform bill, which is aimed at shifting the power to appoint Ukraine's government from the president to the legislature.

In Washington, D.C., US policy makers wondered about the implications of these dual developments. The US relationship with Ukraine (see Map 16.1) was arguably at its lowest point since Ukrainian independence in 1991. A series of shocking revelations about Kuchma's administration—including tape recordings that pointed to Kuchma's involvement in the killing of an investigative journalist and in illegal arms sales to Iraqi leader Saddam Hussein—had badly frayed US–Ukrainian ties, leading Washington to restrict its dealings with Kuchma to a minimum.³ The scheduling of elections raised the prospect that a new president could assume office and turn the page on the relationship's problems. But Kuchma's maneuverings on constitutional reform begged questions about his willingness to let go of power. As they considered how best to chart a course toward more productive relations with Kiev, Washington policy makers turned to analysts for help in understanding how Ukraine's presidential transition might unfold in the fall.

Origins of a Transition

The events of 18 March were but the latest twists in a long-running Ukrainian saga that mixed modern electoral politics with Byzantine court intrigue. Leonid Kuchma was just the second president in Ukraine's short history of post-Soviet independence, and his tenure had been marked by near-constant political ferment. A former Soviet-era industrialist from Ukraine's east, Kuchma had won office in 1994 by amassing 52 percent of the vote in a runoff election against incumbent Leonid Kravchuk, which had divided largely along geographic lines: voters in the Ukrainian-speaking west and center of Ukraine had opted for Kravchuk, while those in the Russian-speaking east and south of the country backed Kuchma. Kuchma's first years in office featured rapid progress in implementing monetary, trade, fiscal, deregulatory, and privatization reforms, with significant assistance from the International Monetary Fund, European Union, US Agency for International Development, and American financier-philanthropist George Soros.⁴ Kuchma and his team of technocrats—including then-chair of Ukraine's National Bank, Viktor Yushchenko—succeeded in stabilizing the country's currency, easing national debt levels, and privatizing significant portions of the economy. Monthly inflation fell from the hyperinflationary level of 91 percent per month in December 1993 to 2.1 percent in the summer of 1994.⁵

Map 16.1 ■ Ukraine



As Ukraine's economy stabilized, however, the struggles for dominance among the country's three power centers—president, prime minister, and legislature—grew more acute. To bolster his power, Kuchma made constitutional reform his next priority, and in 1996 he succeeded in winning approval for a new constitution that gave the presidency the power to nominate the prime minister—subject to legislative approval—and to appoint all government ministers and regional governors. With reinforced executive powers, Kuchma displayed decreasing interest in responding to popular sentiment, and his administration focused less and less on driving reforms and more and more on intrigue and old-fashioned political patronage.⁶

Pipeline Politics

That patronage focused heavily on Ukraine's lucrative natural gas trade. The country had some gas of its own, and it also hosted an extensive network of gas pipelines constructed during the Soviet era that linked Russia's massive gas reserves to markets in Europe. Nearly a quarter of Europe's natural gas consumption—accounting for a large portion of the Russian government's revenues—flowed through pipelines in Ukraine.⁷ This made Ukraine a vital strategic factor in both the European and Russian economies (see Box 16.2). At the same time, as a legacy of the Soviet period, the price of Russian gas flowing into Ukraine varied widely for different customers. Ukraine's residential customers were graced with a highly subsidized price; Ukraine's industry—based largely in its eastern region and heavily dependent on Russian gas to fuel operations—paid a second, higher price; and European customers further down the pipeline paid a third, much higher set of prices. For unscrupulous and politically connected operators in Ukraine, this multitiered pricing scheme allowed the import of cheap gas allegedly for residential use and its subsequent illegal re-export at enormous profit.⁸

Accordingly, control over the energy industry and its attendant revenues became Ukraine's most powerful political currency, eagerly sought by rival clans inside Ukraine and by powerful players in Russia and the West.

The parties who control the Ukrainian oil and gas sector use their positions to block development, to extract economic rent, and to pick commercial winners and losers for their personal convenience. For example, only some projects get governmental approvals;

only some companies get sought-after contracts. Consequently, control over the sector is a major prize in political contests. When one political bloc is uppermost in national politics, no project proceeds without the blessing of, and benefits for, people connected with that bloc. When that group loses the political upper hand, deals are often subject to renegotiation. At the same time, it becomes the job of each successive political opposition to block all policy proposals, even the sensible ones, because the opposition is not profiting.⁹

Box 16.2 UKRAINE THROUGH RUSSIAN EYES

Ukraine at the turn of the millennium was arguably the most important country in the world from the Russian perspective. A series of official Russian foreign policy documents had defined the newly independent former Soviet republics along Russia's periphery as Moscow's top foreign policy priority.ⁱ Ukraine's large population, deeply rooted historical and cultural ties to Russia, and its centrality to Russia's economy made it by far the most prominent state in this category. Nearly a quarter of Moscow's state revenues derived from oil and gas exports to Europe, and some 80 percent of its gas exports to the lucrative European market depended on pipelines crossing Ukraine.ⁱⁱ Short of physical ownership of the pipelines, the Kremlin anxiously sought a regime in Kyiv that would respect vital Russian energy interests. It was therefore not surprising that Moscow had selected one of its most powerful energy titans, ex-prime minister and erstwhile Gazprom chair Viktor Chernomyrdin, as its ambassador to Ukraine in 2001.



Russian President Vladimir Putin (right) with Ukrainian President Leonid Kuchma, March 2002.

Beyond these energy concerns, the unsettled question of Ukraine's geopolitical orientation was a matter of great emotional and practical import for Russia. The North Atlantic Treaty Organization's (NATO) inclusion of Poland, Hungary, and the Czech Republic in 1999 troubled Moscow, which believed the enlargement to be inconsistent with assurances at the time of Germany's unification that NATO would not move eastward. The Russians were powerless to prevent the move, however, and gradually accepted it. By early 2004, NATO was moving rapidly to incorporate seven additional members, including the former Soviet republics of Latvia, Lithuania, and Estonia, and Ukraine was beginning to figure prominently in discussions about a potential third tranche of new members. Russia's relations with the United States—which had warmed following

the attacks of 11 September 2001 as Washington sought help against terrorist groups and their supporters in Iraq, Iran, and elsewhere—began once again to sour after Moscow refused to back the Iraq war and Washington celebrated the triumph of pro-NATO nationalists in Georgia’s “Rose Revolution” (see Box 16.3). The possibility that the NATO alliance could move into the heartland of Moscow’s former empire and assume control of the all-important Ukrainian pipelines prompted deep anxiety in both the security and business establishments in Russia.

i. “The Foreign Policy Concept of the Russian Federation,” June 28, 2000, reprinted at <http://www.fas.org/nuke/guide/russia/doctrine/econcept.htm>.

ii. Radio Free Europe/Radio Liberty, “Factbox: Russian Gas Export Pipelines, Projects,” January 6, 2009, http://www.rferl.org/content/Russian_Gas_Export_Pipelines_Projects/1366873.html.

The high stakes attached to the control of Ukraine’s gas sector made the country’s electoral politics far more than a simple battle for voter support. Behind a façade of party platforms and coalition building, Ukrainian elections intertwined powerful business owners, organized crime, and raw geopolitical maneuvering from abroad with what appeared to be only nominal regard for the legal and ethical norms that constrain electoral behavior in the West. In the run-up to the 1998 parliamentary elections, corrupt industrialists (“oligarchs”) based in the eastern cities of Dnepropetrovsk (including Kuchma’s billionaire son-in-law Viktor Pinchuk) and Donetsk rose to prominence, much to the chagrin of liberals and nationalists in Ukraine’s west.¹⁰ Just as Russian businesspeople had used their wealth and media control to ensure Russian President Boris Yeltsin’s reelection in 1996, so too did Ukrainian businesspeople—working with Viktor Medvedchuk, another prominent oligarch and leader of the Social Democratic United Party—orchestrate Kuchma’s reelection in 1999. He won by a vote of 56 percent to 37 percent in a runoff against Communist Party leader Petro Symonenko.¹¹ Office of Democratic Institutions and Human Rights (OSCE) election monitors criticized that election for numerous improprieties, including “widespread and systematic” campaigning by state officials for Kuchma, violations of Ukraine’s election laws, and comprehensive failure to ensure balanced media coverage.¹² Medvedchuk eventually became Kuchma’s chief of staff during the latter’s second term, and oligarchs based in Ukraine’s east tightened their grip on both politics and commerce.

Box 16.3 GEORGIA’S “ROSE REVOLUTION”

In early November 2003, less than a year before Ukraine’s presidential election was scheduled to take place, Georgia, another former Soviet republic, held legislative elections. The elections were widely viewed as a key test of the strength of contending political factions prior to the Georgian presidential election slated for the spring of 2005, when the increasingly unpopular president Eduard Shevardnadze was due to leave office.

The election pitted government loyalists, who controlled Georgia’s commerce and media, against self-proclaimed liberals attempting to exploit the public’s growing unhappiness with perceived bureaucratic corruption. Official results indicated that Shevardnadze’s ruling party triumphed, but opposition groups alleged massive fraud in the

vote tabulation. Citing independent exit polls, Mikheil Saakashvili, a US-educated former Georgian official who had gone into political opposition after a falling out with Shevardnadze, claimed that his party had in fact won the elections, and he urged Georgians to undertake a campaign of public demonstrations and nonviolent civil disobedience against Shevardnadze's regime.



Rallying around Saakashvili's claims, Georgia's main opposition parties united to demand Shevardnadze's ouster and the rerun of the elections. In mid-November, massive anti-government demonstrations erupted in the central streets of Tbilisi, and they soon spread to nearly all of Georgia's major cities. A youth organization called *Kamara* ("Enough!") and several prominent nongovernmental organizations (NGOs) helped to organize the protests, which reached their peak on 22 November, when Shevardnadze attempted to open the new session of the parliament. Led by Saakashvili, protesters burst into the session with roses in their hands, prompting Shevardnadze to flee the building. He declared a state of emergency and attempted to mobilize military and security forces, but they refused to support the government. Recognizing the inevitable, Shevardnadze reached out to opposition leaders Saakashvili and Zurab Zhvania on 23 November in a meeting arranged by then-Russian foreign minister Igor Ivanov. After the meeting, Shevardnadze announced his resignation. New presidential elections were held in January 2004, in which Saakashvili won an overwhelming victory.

NGOs had played a significant role in monitoring the parliamentary elections, organizing opposition groups and protesters, and financing their activities. A former Georgian parliamentarian claimed that in the three months prior to the Rose Revolution, the Soros foundation had spent some \$42 million in support of Georgian NGOs.ⁱ Soros himself downplayed the role of his foundation in the Rose Revolution, however, saying that he was "pleased and proud of the work of the foundation in preparing Georgian society for what became a Rose Revolution," but that "the role of the foundation has been greatly exaggerated."

i. K. R. Bolton, "Russo-Georgian Conflict Originates with Soros Subversion," August 14, 2008, <http://www.rense.com/genera183/soros.htm>.

A House Divided

The rough and tumble of gas politics produced an array of victims as well as victors, however. Viktor Yushchenko became prime minister under Kuchma at the end of 1999, but following his attempts to reform the energy sector, he was removed in 2001 by a Rada vote of no confidence that was initiated by Kuchma's oligarchic allies; his firing transformed him from mere technocrat into an opposition politician with a strong public base.¹³ Similarly, Yulia Tymoshenko made millions from the gas trade in the 1990s through a shady alliance with then-deputy prime minister Pavel Lazarenko (whom the United States subsequently convicted of money laundering), and she parlayed her wealth into political prominence as deputy prime minister for fuel and energy in the early years of Kuchma's second term.¹⁴ But after tangling with some powerful oligarchs, she found herself fired from the government in 2001 and then briefly jailed on charges of corruption levied by both Ukrainian and Russian prosecutors.¹⁵ Emerging from prison after the Kuchma government dropped the charges, she entered opposition politics with a vengeance, leading a series of popular demonstrations against the Kuchma regime's corruption and cozy dealings with Russia.¹⁶

The opposition's criticisms resonated with significant portions of Ukraine's public. In late 2000, a former Kuchma bodyguard released a series of tapes that he claimed to have secretly recorded. The tapes documented Kuchma's involvement in the killing of an investigative journalist and in the illegal sale of arms to Iraqi leader Saddam Hussein. The tapes became a sensation, and they fed a growing perception that there was little that Kuchma and his oligarchic allies would not do to amass and protect their wealth and political power.¹⁷ Several prominent businesspeople broke with the Kuchma regime, fed up with the government's heavy-handed efforts to control their operations.¹⁸ A study by the US-based nonprofit International Foundation for Election Systems conducted at the end of 2003 found that 85 percent of Ukrainians were either very or somewhat dissatisfied, and a similar percentage felt that corruption was a common and serious problem; 70 percent had little or no confidence in Kuchma.¹⁹

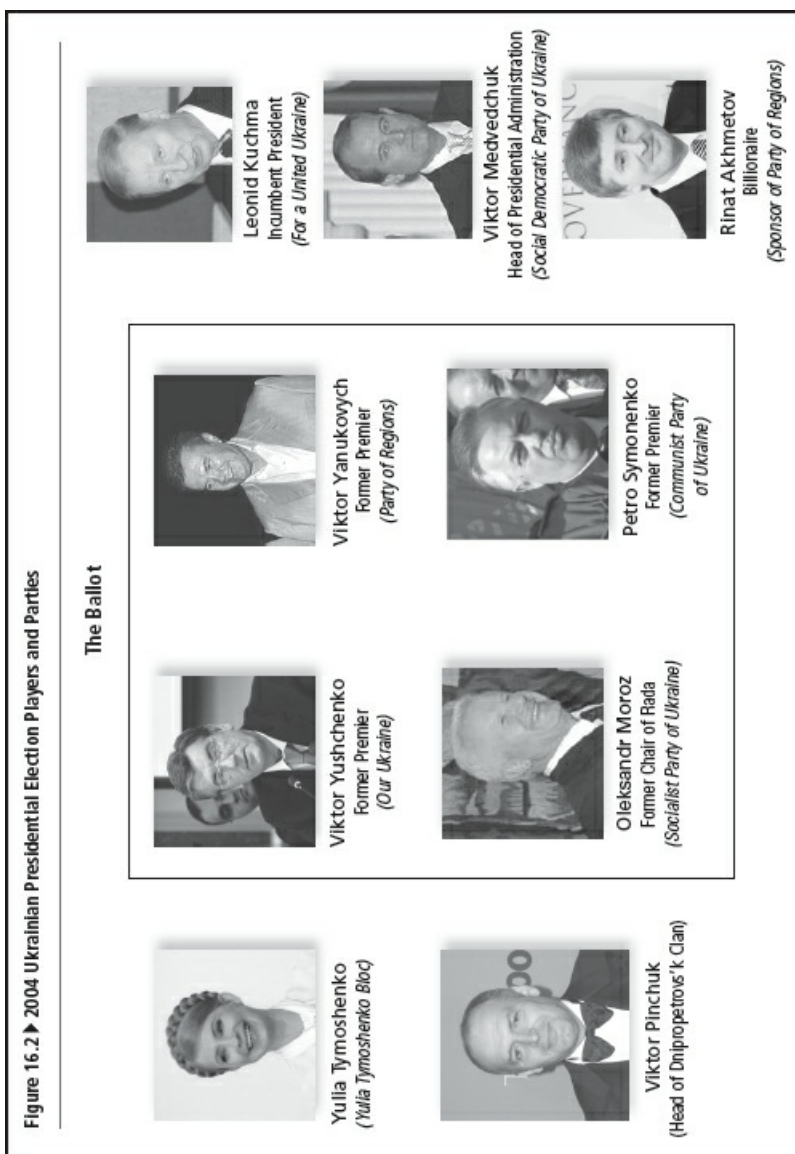
These perceptions redounded to the advantage of Ukraine's political opposition. Determined to capitalize on popular discontent and avoid the squabbling that had plagued oppositionists in the past, former prime minister Viktor Yushchenko formed a broad umbrella group, "Our Ukraine," that united centrist and rightist opposition forces and swept to victory in the 2002 parliamentary elections, amassing nearly a quarter of the vote.²⁰ Kuchma chief of staff Medvedchuk employed numerous tactics to thwart the opposition—for example, denying Yushchenko coverage by state-controlled media and hiring Russian political consultants to set up fake parties to draw support from actual opposition groups—but the pro-government bloc won a paltry 11.8 percent of the vote.²¹

Marshaling of Forces

Defeat in the 2002 parliamentary elections sent a jolt through Kuchma's administration. As his second term as president neared its end, Kuchma and his team of political operators suddenly faced the danger of losing not only their offices but also their freedom, should the next president prosecute them for any of the numerous crimes that they had allegedly committed. To address this danger, they pursued several options. Immediately following the elections, Medvedchuk moved quickly and effectively to bribe or intimidate legislators into supporting the regime, and Kuchma subsequently initiated a new round of constitutional reforms designed to transfer several

executive authorities from the presidency to the Rada, where his allies could presumably continue to wield power behind the scenes.²² Following the Constitutional Court's ruling on 18 March 2004 that the reform bill was constitutional, the bill faced just one more hurdle: approval by a two-thirds majority in the legislature.

In addition to pursuing constitutional reform, Kuchma also attempted to engineer the election of a loyal successor. After much deliberation, Kuchma settled on Viktor Yanukovych, the hardscrabble governor of the crime-ridden Donetsk region, leader of the Regions of Ukraine party, and reputed protégé of Ukraine's richest and most brutal oligarchic clan, headed by Rinat Akhmetov.²³ Kuchma named Yanukovych as prime minister in November 2002, signaling all but explicitly that he would be the regime's preferred candidate in the 2004 presidential election. In support of Yanukovych's candidacy, Medvedchuk tightened the regime's control over broadcast media and the Central Electoral Commission.²⁴ Together with Ukraine's top oligarchic clan leaders, Medvedchuk began planning the most expensive presidential campaign in Ukraine's history, funded heavily by Akhmetov.²⁵



Meanwhile, the other “Viktor”—Yushchenko—emerged as Yanukovych’s primary opposition for the presidency. Handsome and articulate, Yushchenko stood in sharp contrast to the hulking and poorly spoken Yanukovych, and opinion polls consistently ranked him as Ukraine’s most popular politician. Still, he faced a formidable battle to succeed Kuchma. Denied the airwaves, he focused on organizing large public rallies, covered by Ukraine’s newly emerging Internet newspapers.²⁶ Uniting centrist and nationalist opposition groups behind him, Yushchenko targeted the support of Ukraine’s “multimillionaires”—conceding that its billionaires would back Yanukovych—and centered his campaign on the themes of good government, good values, private property, and European integration.²⁷ As Ukraine’s long winter melted into the spring of 2004, analysts weighed his prospects for success against the combined efforts of Ukraine’s wealthiest and most powerful forces.

RECOMMENDED READINGS

International Foundation for Election Systems. “Attitudes and Expectations: Public Opinion in Ukraine 2003.”
http://www.ifes.org/~media/Files/Publications/Survey/2004/142/Ukraine_Survey_2003_Eng
Office of Democratic Institutions and Human Rights (OSCE). “Ukraine Presidential Elections 31 October and 14 November 1999 Final Report.” Warsaw, Poland: March 7, 2000.
Pifer, Steven. “Ukraine’s Future and US Interest.” House International Relations Committee Subcommittee on Europe, May 12, 2004. <http://2001–2009.state.gov/p/eur/rls/rm/32416.htm>.

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

SHADES OF ORANGE IN UKRAINE

Structured Analytic Techniques in Action

The exercises in this case require you to put yourself in the shoes of an analyst who has just been tasked by the US National Security Council to provide an assessment of the factors that will determine who the next Ukrainian president will be. Policy makers often call on analysts in this manner to support policy deliberations in advance of major policy initiatives. In this case, the Ukrainian election is still months away, and US policy makers are grappling with how best to ensure that Ukraine holds a free and fair election. Analysts can add tremendous value by helping policy makers understand the full complement of factors that will determine who will be the next Ukrainian president. This type of analysis can help policy makers identify opportunities for pursuing US interests and avoid potential pitfalls.

Techniques 1 and 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.

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).

Using these two techniques together prompts analysts to consider the full range of factors that could shape the outcome of the election.

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.

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.

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.

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.

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.

STEP 8: When all sticky notes have been arranged, ask the group to select a word or phrase that best describes each grouping.

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.

Analytic Value Added. What key factors will influence the outcome of the election? What gaps deserve additional attention?

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.

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.

STEP 2: Make a list of forces, factors, and events that are likely to influence the future.

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.

STEP 4: Write a brief description of each or use the descriptions previously developed.

STEP 5: Generate a matrix with the list of drivers down the left side, as shown in Table 16.2.

Table 16.2 ▶ Simple Scenarios Template

	Best Case	Worst Case	Mainline	Additional
Driver 1				
Driver 2				
Driver 3				
Driver 4				
Driver 5				

STEP 6: Generate at least four different scenarios: a best case, a worst case, mainline, and at least one other.

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?

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.

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.

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.

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?

NOTES

1. Radio Free Europe/Radio Liberty, *Newsline*, March 18, 2004, <http://www.rferl.org/content/article/1143120.html>.
2. Radio Free Europe/Radio Liberty, *Newsline*, March 19, 2004, <http://www.rferl.org/content/article/1143121.html>.
3. Tara Kuzio, “US–Ukraine Relations Will Not Revive under Kuchma,” *Kyiv Post*, March 13, 2003, http://www.taraskuzio.net/media21_files/18.pdf; Tara Kuzio, “Ukraine’s Relations with the West: Disinterest, Partnership,

Disillusionment,” *European Security* 12, no. 2 (2003): 21–44, http://www.taraskuzio.net/International%20Relations_files/ukraine_west_relations.pdf.

4. Anders Åslund, “Leonid Kuchma’s Reforms: 1994–96,” chap. 3 in *How Ukraine Became a Market Economy and Democracy* (Washington, DC: Peter G. Peterson Institute for International Economics, 2009), 59–90.

5. Ibid., 73.

6. Ibid., 86.

7. Radio Free Europe/Radio Liberty, “Factbox: Russian Gas Export Pipelines, Projects,” January 6, 2009, http://www.rferl.org/content/Russian_Gas_Export_Pipelines_Projects/1366873.html.

8. Edward Chow and Jonathan Elkind, “Where East Meets West: European Gas and Ukrainian Reality,” *Washington Quarterly* 32, no. 1 (2009): 77–92, http://www.twq.com/09winter/docs/09jan_ChowElkind.pdf.

9. Ibid., 81.

10. Taras Kuzio, “How the Gas Issue Plays in Ukrainian Politics and How Ukrainian Politicians Play the Gas Issue,” transcript from lecture at Harvard University, March 7, 2008, http://www.taraskuzio.net/conferences2_files/Ukrainian_Politics_Energy.pdf.

11. Ibid.

12. Organization for Security and Co-operation in Europe (OSCE), Office of Democratic Institutions and Human Rights (ODIHR), *Ukraine Presidential Elections 31 October and 14 November 1999: Final Report* (Warsaw, Poland: OSCE ODIHR, 2000), http://www.osce.org/odihr/elections/ukraine/presidential_1999/.

13. Taras Kuzio, “Ukraine Steps Up the Struggle against Organized Crime and Corruption—or Does It?” *Radio Free Europe/Radio Liberty Organized Crime and Terrorism Watch* 3, no. 10 (2003), http://www.taraskuzio.net/media11_files/4.pdf; Adrian Karatnycky, “Ukraine’s Orange Revolution,” *Foreign Affairs*, March–April 2005, <http://www.foreignaffairs.com/articles/60620/adrian-karatnycky/ukraines-orange-revolution/>.

14. Irena Chalupa, “Ukraine’s Gold-Plaited Comeback Kid,” Radio Free Europe/Radio Liberty, September 23, 2008, http://www.rferl.org/content/Tymoshenko_Profile/1291005.html.

15. Roman Woronowycz, “Yulia Tymoshenko Arrested,” *Ukraine Weekly*, February 18, 2001, <http://www.ukrweekly.com/old/archive/2001/070107.shtml>.

16. Chalupa, “Ukraine’s Gold-Plaited Comeback Kid.”

17. Åslund, *How Ukraine Became a Market Economy and Democracy*, 154.

18. Ibid.

19. Rakesh Sharma and Nathan Van Dusen, *Attitudes and Expectations: Public Opinion in Ukraine 2003* (Washington, DC: International Foundation for Election Systems, 2004), http://www.ifes.org/~media/Files/Publications/Survey/2004/142/Ukraine_Survey_2003_English.pdf.

20. Central Election Commission of Ukraine, <http://www.cvk.gov.ua/>.

21. Åslund, *How Ukraine Became a Market Economy and Democracy*, 155–56.

22. Olexiy Haran and Rostyslav Pavlenko, “Political Reform or a Game of Survival for President Kuchma?” PONARS (Program on New Approaches to Russian Security) Policy Memo 294, November 2003, http://www.gwu.edu/~ieresgwu/assets/docs/ponars/pm_0294.pdf; Åslund, *How Ukraine Became a Market Economy and Democracy*, 158–59.

23. Taras Kuzio, “From Kuchma to Yushchenko,” *Problems of Post-Communism* (March/April 2005), 8, http://www.taraskuzio.net/Comparative%20Politics_files/electionsorangerevolution.pdf.

24. Åslund, *How Ukraine Became a Market Economy and Democracy*, 180.

25. Ibid.

26. Ibid., 178.

27. Ibid., 179.

17 Violence Erupts in Belgrade

Key Questions

- ▶ Who targeted the US presence in Belgrade, and why?
- ▶ What could increase or decrease the threat of future violence?
- ▶ What competing interests must the United States weigh when deciding how to respond to anti-American violence?

CASE NARRATIVE

On the evening of Sunday, 17 February 2008, an angry crowd of several hundred Serbian protesters converged on the US Embassy building—or Chancery—in Belgrade, Serbia. The mob threw stones at the building, chanted nationalist slogans, and vented anger at US support for Kosovo’s declaration of independence from Serbia earlier in the day.¹ With some difficulty, Serbian police repelled the attacks, but not before the rioters had assaulted and damaged the US, Croatian, and Slovenian embassies, as well as McDonald’s and Nike stores nearby.² Serbian officials downplayed the attacks and emphasized Serbia’s commitment to peaceful resolution of the situation surrounding Kosovo.³ But violence in the Serbian capital, coupled with sporadic eruptions in neighboring Kosovo, forced US officials to make difficult assessments about the prospective threat to US interests in the region and how the United States should respond. Did these attacks presage greater violence against Americans, and should US officials count on Serbian authorities to protect the US diplomatic presence?

Another Chapter in an Epic Struggle

The violence on 17 February was but the latest episode in the bloody and emotion-laden conflict over Kosovo that has waxed and waned for centuries. Albanians have deep roots in the region, claiming to be direct descendants of the Illyrians, the earliest known inhabitants of Kosovo. For Serbs, Kosovo has long had great symbolic importance as the host of several revered Orthodox shrines. It is also the site of Serbia’s defeat at the hands of the Turks in the “Battle of Kosovo Polje” in 1389, which led to Serbia’s subjugation to the Ottoman Empire until its independence in 1898. Under Ottoman rule, the Albanian population in Kosovo grew dominant and the majority converted to Islam, while much of the Orthodox Serbian population moved northward toward Belgrade in the so-called Great Migration.⁴



Serbian riot police block a street during clashes with protesters in front of the US Embassy in Belgrade, 17 February 2008.

In the course of the seventeenth, eighteenth, and nineteenth centuries, Kosovo and the rest of the Balkans became an arena for conflict between empires (Ottoman, Austro-Hungarian, and Russian) and religions (Islam, Catholicism, and Orthodox Christianity). By the turn of the twentieth century, these conflicts had assumed an ethnic character, as both Serbian and Albanian nationalists struggled to carve new nation-states out of the decaying Ottoman Empire and assert control over Kosovo. Vicious fighting between Serbs and Albanians broke out repeatedly, with multiple allegations of massacres by each side against the other. After changing hands numerous times prior to the end of World War II, Kosovo became an integral part of the republic of Serbia within Yugoslavia.⁵

During Communist rule under Yugoslav leader Josip Broz Tito, the Albanian population of Kosovo grew rapidly until it exceeded three-quarters of the region's inhabitants, while the Slav population dwindled to less than a sixth. A powerful Albanian national movement prompted Tito to grant Kosovo autonomy in 1974, fueling Serbian nationalist resentment that Serbian Communist Party chief Slobodan Milosevic rode to power. In 1989, he revoked Kosovo's autonomy, and as Yugoslavia disintegrated in the early 1990s, he banned the Albanian language from official use and fired Albanians employed in public institutions who would not take an oath of allegiance to the Federal Republic of Yugoslavia (FRY). Kosovar Albanians responded with numerous protests, strikes, and the establishment of extra-legal parallel government institutions, setting the stage for direct confrontation between Kosovar Albanians and Serbian authorities in what was then the FRY.⁶

By 1998, this confrontation had escalated into de facto civil war between Kosovar Albanians and Serbs. An increasingly well-armed and well-funded underground Albanian guerrilla movement, the Kosovo Liberation Army, emerged from the shadows and launched a series of operations against Serbian officials and civilians in Kosovo. Milosevic responded ruthlessly, killing more than fifteen hundred Kosovar Albanians, driving more than four hundred thousand from their homes, and engaging in what the Organization for Security and Co-operation in Europe (OSCE) called "a pattern of human rights and humanitarian law violations on a staggering scale, often committed with extreme and appalling violence."⁷

Diplomatic efforts to resolve the conflict by the United Nations (UN), OSCE, and six-nation

“Contact Group” (United States, Russia, France, Italy, United Kingdom, and Germany) had little impact, in part because of Russia’s reluctance to enforce international dictates on what it regarded as a domestic Yugoslav affair. As the fighting continued to escalate, the North American Treaty Organization (NATO) alliance issued a warning to both sides and announced its willingness to use air strikes if necessary to end the fighting. NATO’s initiative culminated in negotiations in Rambouillet, near Paris, in February and March 1999, where the Kosovar Albanian delegation signed a proposed peace agreement but the Serbian delegation refused. Immediately afterward, FRY military and police forces stepped up operations against ethnic Albanians in Kosovo.⁸

Having failed to persuade Milosevic to stop the attacks, NATO commenced air strikes on 23 March 1999. The bombing—which targeted not only the Yugoslav military but also strategic assets such as electrical grids, water facilities, and communications infrastructure—continued until 10 June, when, with Russian mediation, NATO and Yugoslav authorities announced a military-technical agreement to end hostilities. This was followed in short order by the passage of UN Security Council Resolution (UNSCR) 1244, which placed Kosovo under interim UN administration, authorized a NATO-led peacekeeping force (KFOR), affirmed the territorial integrity and sovereignty of the FRY (now Serbia), and initiated a political process to determine Kosovo’s future status. Although the UN resolution effectively ended the fighting, it did not end the dispute over Kosovo: violence between the remaining Serbian enclaves and Kosovar Albanians flared periodically, and in 2004 riots erupted that resulted in widespread attacks by crowds of Albanians on Serb communities and cultural sites.⁹

The hard task of reconciling competing Albanian and Serbian claims over Kosovo’s status fell to the respected Finnish politician and diplomat Martti Ahtisaari, who in late 2005 was appointed UN special envoy for Kosovo. After more than a year of status negotiations, Ahtisaari produced a draft settlement proposal that could serve as the basis for an eventual agreement. The package he presented to the UN Security Council in April 2007 included a recommendation that Kosovo become independent subject to a period of international supervision. (See Map 17.1.) Kosovar Albanians accepted the proposal; Serbia rejected it as a violation of its legal sovereignty over Kosovo, which it argued was reaffirmed by UNSCR 1244. The United States and European Union (EU) supported the Ahtisaari plan and Kosovo’s push for independence. Russia backed Belgrade’s position, rejected a draft UN Security Council Resolution based on the Ahtisaari plan, and called for new negotiations to produce a settlement acceptable to both sides.¹⁰

February 2008: Tense Final Days of the Impasse

By February 2008, Kosovar Albanian patience with the impasse was reaching its end (see Figure 17.1). A unilateral declaration of independence by Kosovo appeared imminent. In Kosovo, posters emblazoned with the US, British, and EU flags expressed thanks “to all the countries [that] are contributing [to] and supporting the independence of Kosovo.”¹¹ Other posters around the capital of Pristina urged Kosovar Albanians to “celebrate with dignity.”¹² Serbian Prime Minister Vojislav Koštunica—amid reports that the European Union was considering a plan to send a police force to Kosovo post-independence—reiterated that Serbia would never accept Kosovo’s independence, and he accused Europe, “under strong outside pressure from the US,” of “trampling [on] the fundamental principles” of the United Nations as the European Union “yielded to a policy of force.” Serbian President Boris Tadic, however, in a nod toward Serbian hopes for EU membership, tempered his comments, saying, “I will never give up the fight for

our Kosovo, and with all my strength, I will fight for Serbia to be in the European Union.”¹³ Ethnic tensions inside Kosovo seemed to mount; police in Kosovo’s ethnically divided city of Mitrovica reported an explosion behind a building that housed the advance team for the EU mission.¹⁴ The next day, the European Union approved a plan to send an eighteen-hundred-person police and judicial mission to help Kosovo’s nascent government.¹⁵

Map 17.1 ▀ Serbia and the Breakaway Republic of Kosovo



Figure 17.1 ▀ February 2008: Kosovo Status at an Impasse



In Serbia, the government braced for the inevitable and adopted an action plan pledging no violence and a resolution preemptively declaring any unilateral act by Kosovo's ethnic Albanian leadership to be invalid and illegal. Koštunica enjoined Serbians to reject Kosovo's independence, saying, "We shall not allow such a creation to exist for a minute. It has to be legally annulled the moment it is illegally proclaimed by a leadership of convicted terrorists."¹⁶ Its annulment was planned to be the centerpiece of a "Thursday of rejection" planned for 14 February.¹⁷

Reports surfaced about an alleged Serbian "secret action plan" to be implemented upon Kosovo's declaration of independence, which reportedly included retaliatory steps to keep Kosovo under Serbian control.¹⁸ Publicly, however, Serbian Foreign Minister Vuk Jeremic told the UN Security Council that although Serbia would never accept a violation of its territorial integrity and would take diplomatic, political, and economic measures to impede Kosovo, Belgrade would not use force to keep Kosovo from seceding.¹⁹

The Day of the Attack

Braving heavy snow and freezing temperatures, Kosovar Albanians on 17 February took to the streets to celebrate their parliament's vote for independence with festive rallies, fireworks, and even a hundred-foot birthday cake. Some revelers waved US flags and chanted "God Bless America."²⁰

In Belgrade, the mood was far less joyous. In a fiery, nationally televised speech just minutes after Kosovo's declaration, Koštunica declared Kosovo's independence null and void and denounced the United States and European Union for supporting Kosovo's secession.²¹ In addition to accusing Washington of being "ready to violate the international order for its own interests," Koštunica singled out US President George W. Bush for personal rebuke, saying that he "is responsible for this violation, [and] will be noted in black letters in Serbian history books, along with his European followers."²² Despite the acerbic remarks, Serbian leaders pledged peaceful resistance after Kosovo's declaration.²³ In Kosovo, however, unidentified attackers threw grenades at EU and UN buildings, and Serbs who had gathered to protest the declaration

said they were under orders from Belgrade to ignore the independence declaration and remain in Kosovo to keep the northern part of the territory under de facto Serbian control.²⁴

By evening, violence threatened in Belgrade as protesters gathered at the US Chancery. Pre-positioned Serbian riot police guarded the building—which directly abuts the sidewalk and a major thoroughfare—but the protesters grew quickly in numbers and fury. They chanted, “Kosovo is the heart of Serbia,” as they hurled paving stones, rocks, and bottles at police. The scene outside the Chancery grew particularly tense as the rioters threw incendiary devices at the building façade and tried to push past Serbian antiriot police.²⁵ The police eventually drove the rioters back from the building, but the angry mob only turned its attention to ransacking and burning a nearby McDonald’s. The crowd also targeted other Western embassies, including those of NATO member Turkey and EU member Slovenia; the latter had recently taken over the EU chairmanship.²⁶ Although police prevented a group of rioters from approaching the Albanian Embassy, and none of the seventy diplomats stationed at the US Embassy were injured, more than thirty people were wounded in the riots.²⁷ (See Box 17.1 for a discussion of US Embassy security.)



The US Embassy building in Belgrade guarded by Serbian police, 17 February 2008.

Box 17.1 PROTECTING US DIPLOMATIC MISSIONS

The February 2008 attack on the US Embassy building in Belgrade was not the first time that the United States has faced threats to its interests in Serbia. In March 1999, just before NATO commenced bombing, the United States severed diplomatic relations and completely closed its embassy in Serbia. The United States did not formally reopen the embassy until May 2001.ⁱ

In nonemergency situations, the downgrading of bilateral relations is often preceded by the political step of withdrawing the ambassador or highest-ranking diplomat, often at least initially “for consultations,” to a country’s home capital. But the severing of diplomatic relations and closing of an embassy are rare and usually are reserved for extraordinary circumstances such as war or serious civil instability. The United States

instead works to maintain its representation abroad, even in dangerous locales. To protect the safety of its diplomats and their families, the United States often will designate a particularly dangerous environment an “unaccompanied post,” where diplomats must live and work without their families. This is true for the wartime embassies in Baghdad, Iraq, and Kabul, Afghanistan. Under normal circumstances, however, the families of US diplomats do accompany their family member to the post, even if the security situation has been tenuous in the past.

In the face of a sudden change in the security environment, the United States must carefully calibrate its response to protect US interests, personnel, and property. For example, in 2010 the United States for several days temporarily closed, rather than evacuated, its embassy in Yemen in response to specific threats by al-Qaeda in the Arabian Peninsula (AQAP) to attack American interests in Yemen.ⁱⁱ Closures such as these do not come without a financial cost, which must be weighed against the threat, but US officials at the time said the specificity of the threat warranted this “administrative closure” to protect US Embassy personnel. Other countries, whose embassies in Yemen were not specifically threatened, such as France and Spain, also closed their embassies to public access but kept their administrative offices open.

There are some circumstances in which evacuation—ranging from voluntary through dependents only, nonessential personnel, and full mandatory evacuation—are deemed necessary to protect US persons. Following a 2010 attack in Mexico in which US personnel and dependents were killed, the United States offered staff the option of voluntary temporary evacuation of dependents but kept its Chancery and consulates open.ⁱⁱⁱ

Decisions about security are made by the ambassador, in consultation with embassy staff and the Department of State, particularly if a security issue threatens bilateral relations between the two countries. If the ambassador is absent, the deputy chief of mission is designated to act as *chargé d'affaires*. An embassy’s physical security is maintained by the Regional Security Officer (RSO) and the Marine Security Guard Detachment (MSG) assigned to the embassy. The MSG is responsible for interior security of the post, including access control, personnel protection, and protection of sensitive classified information and equipment.^{iv} The MSG reports to the ambassador through the RSO. In times of heightened tension in which the embassy is temporarily closed, the MSG, RSO, and other core staff will continue to maintain on-site security. Exterior security is governed by the 1961 Vienna Convention on Diplomatic Relations, which established the inviolability of the foreign mission and the receiving state’s “duty to take all appropriate steps to protect the premises of the mission against any intrusion or damage and to prevent any disturbance of the peace of the mission or impairment of its dignity.”^v

i. “Background Note: Serbia,” US Department of State, <http://www.state.gov/r/pa/ei/bgn/5388.htm>.

ii. Julian Borger, Hugh Macleod, Ed Pilkington, and Peter Walker, “US and UK Keep Yemen Embassies Shut for Second Day,” *Guardian* (London), January 4, 2010, <http://www.guardian.co.uk/world/2010/jan/04/yemen-embassies-shut/>.

iii. “3 People Associated with US Consulate Killed in Mexico,” CNN, March 14, 2010, http://articles.cnn.com/2010-03-14/world/mexico.violence_1_detention-officer-police-officer-sheriff-s-office.

iv. Michael Coady, “A Salute to Marine Security Guards,” *DIPNOTE* (US Department of State blog), November 11, 2009, http://blogs.state.gov/index.php/entries/salute_marine_security_guards/.

The Aftermath

On 18 February 2008, despite fears that formal Western recognition of Kosovo's independence would spark a new round of violence in Belgrade and Kosovo, the United States formally recognized Kosovo's independence.²⁸ France, the United Kingdom, Turkey, and over a dozen other EU and NATO countries quickly followed suit.²⁹ Serbia protested the move by recalling its ambassador from Washington, D.C., and from other states that recognized Kosovo, but it did not sever diplomatic relations with the United States.³⁰

On Monday and Tuesday, the celebrations in Pristina did not let up, but neither did the opposition and ensuing violence. Several thousand Serbs on Monday marched across the river dividing the ethnic Serbian northern portion of the city of Mitrovica from its ethnic Albanian south, chanting, "Kosovo is Serbia." On Tuesday, Kosovo Serbs set fire to the Jarinje and Banja crossings on Kosovo's border with Serbia. The attack destroyed cars and burned small buildings, but there were no injuries. NATO and UN authorities closed the border in response.³¹ (See Figure 17.2 for a chronology of events.)

Figure 17.2 ► Chronology of Selected Events

Date	Event
1974	Josip Broz Tito grants Kosovo autonomy.
1989	Slobodan Milosevic revokes Kosovo autonomy.
1990s	Yugoslavia disintegrates, but Kosovo remains integrated.
1998	Kosovar Albanians protest lack of independence and set up a parallel government. A de facto civil war breaks out between Kosovar Serbs and Albanians.
March 1999	NATO sponsors the Rambouillet Conference at which Kosovar Albanians sign a peace agreement, but the Serbs refuse. US-led NATO airstrikes mark beginning of war; Washington officially severs diplomatic relations with Serbia and closes its embassy.
June 1999	NATO and Serb authorities—with Russian mediation—announce a military-technical agreement to end hostilities, and the United Nations passes UN Security Council Resolution (UNSCR) 1244.
May 2001	The United States formally reopens Embassy Belgrade.
2005	Martti Ahtisaari is appointed UN Special Envoy for Kosovo.
April 2007	Ahtisaari presents a package to the UN Security Council that includes a recommendation that Kosovo become independent subject to a period of international supervision. Kosovar Albanians accept the proposal; Serbia rejects it as a violation of its legal sovereignty over Kosovo, which it argues was reaffirmed by UNSCR 1244.
13 February 2008	Serbian National Council meets and rejects in advance Kosovo independence, adopts action plan, and rules out nondiplomatic retaliatory steps such as military intervention or disruption of electricity.
15 February 2008	Boris Tadic is sworn in as Serbian president.
16 February 2008	European Union announces plan to send eighteen-hundred-strong police and judicial force to Kosovo.
17 February 2008	Kosovo declares independence. Russia calls UN Security Council emergency session. Anti-independence rally in Belgrade turns violent, and “hooligans” attack US Embassy.
18 February 2008	The United States recognizes Kosovo independence. Rallies and additional riots break out in Belgrade. Serbia recalls its ambassador from the United States.
19 February 2008	Attacks occur on UN-monitored border posts Jarinje and Banja in northern Kosovo.

Observers’ fears about further violence in Belgrade were proved at least partially correct when new protests resulted in small incidents of violence around the city on Monday. Police cordons prevented rioters from approaching Belgrade’s “embassy row,” where many Western embassies are located, and the protesters resorted to throwing stones at the officers. Elsewhere, rioters vandalized another McDonald’s and the Turkish Embassy, and police evacuated a shopping mall after a bomb threat.³²

Newspaper headlines in Belgrade on Tuesday morning trumpeted defiance and anger over international support for Kosovo’s declaration. Reports indicated that Koštunica and other party leaders planned to address a government-supported protest rally on Thursday, but Tadic demurred and scheduled a trip to Bucharest to thank Romania for its refusal to recognize Kosovo. Tadic, who had just been in New York to address the UN Security Council, appealed for calm ahead of the rally, urging that “there must be no violence and endangering of human lives . . . [because] only peace and reasonable moves give us the right to defend Kosovo.”³³ The United States acknowledged that “small demonstrations” in Belgrade continued and expressed gratitude to the Serbian government for “maintaining law and order . . . and security around [the

US] Embassy.”³⁴ Nevertheless, with the clock ticking on the state-sponsored “Kosovo is Serbia” rally, the United States scrambled to calculate whether the rally might turn violent and how the embassy should prepare for it.

RECOMMENDED READINGS

Glenny, Misha. *The Balkans: Nationalism, War, and the Great Powers, 1804–1999*. New York: Penguin, 1999.

Judah, Tim. *The Serbs: History, Myth, and the Destruction of Yugoslavia*. 3rd ed. New Haven, CT: Yale University Press, 2009.

Malcolm, Noel. *Kosovo: A Short History*. New York: New York University Press, 1998.

Vickers, Miranda. *The Albanians: A Modern History*. London: I. B. Tauris, 2006. Originally published 1995.

Vienna Convention on Diplomatic Relations, 1961. April 18, 1961; entered into force on April 24, 1964. *United Nations, Treaty Series*, Vol. 500 (2005): 95.

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

VIOLENCE ERUPTS IN BELGRADE

Structured Analytic Techniques in Action

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.

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

STEP 3: Make one list showing the strongest forces for and against additional violence.

STEP 4: Array the lists in a table (see the template in Table 17.2).

Table 17.2 ▶ Force Field Analysis Template

Forces for and against Outcome			
Score	Driving Forces	Constraining Forces	Score
Score of 1–5	Driving Force 1	Constraining Force 1	Score of 1–5
Score of 1–5	Driving Force 2	Constraining Force 2	Score of 1–5
Sum of Driving Forces			Sum of Constraining Forces

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.

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.

STEP 8: Analyze the lists to determine how changes in factors might affect the overall outcome.

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?

Analytic Value Added. Is additional violence against US interests in Belgrade likely?

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.

STEP 2: List the selection criteria and options. The number of criteria and options can vary from case to case.

STEP 3: Consolidate items within each list to eliminate overlap among the items.

STEP 4: Fill in a matrix like the example in Table 17.3 with the criteria and options you have generated.

Table 17.3 ► Decision Matrix Template									
Selection Criteria	% Weight (W)	Option 1		Option 2		Option 3		Option 4	
		Value (V)	Weighted Value (W × V)	Value (V)	Weighted Value (W × V)	Value (V)	Weighted Value (W × V)	Value (V)	Weighted Value (W × V)
Criterion 1	30	3.5	105	2.0	60	2.0	60	2.5	75
Criterion 2	10								
Criterion 3	40								
Criterion 4	20								
Weighted Value Totals			105		60		60		75

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.

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.

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.

STEP 9: Use a qualitative sanity check to help identify key issues, variables, or other observations that could further aid the decision-making process.

Analytic Value Added. Based on your findings, which option best protects US political and security interests in Belgrade, and why?

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.

Table 17.4 ▶ Pros-Cons-Faults-and-Fixes Template

Faults	Pros	Cons	Fixes
Describe any faults for Pro 1	Pro 1	Con 1	Describe any fixes for Con 1
Describe any faults for Pro 2	Pro 2	Con 2	Describe any fixes for Con 2
Describe any faults for Pro 3	Pro 3	Con 3	Describe any fixes for Con 3

STEP 1: Clearly define the proposed action or choice.

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.

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.

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.

STEP 6: Compare the Pros, including any Faults, against the Cons 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?

NOTES

1. Dejan Anastasijevic, "Joy in Kosovo, Anger in Serbia," *Time*, February 17, 2008, <http://www.time.com/time/world/article/0,8599,1714164,00.html>.

2. "Rioters Attack US Embassy in Belgrade after Kosovo Protest Rally," Radio Free Europe/Radio Liberty, February 21, 2008, <http://www.rferl.org/content/article/1079512.html>.

3. Ellie Tzortzi, "Serbia Pledges Long-Haul Fight over Kosovo," Reuters, February 17, 2008, http://www.reuters.com/article/2008/02/17/idUSL17718644_CH_2400.

4. Misha Glenny, *The Balkans: Nationalism, War, and the Great Powers, 1804–1999* (New York: Penguin, 1999).

5. Noel Malcolm, *Kosovo: A Short History* (New York: New York University Press, 1998).

6. Gordon N. Bardos, "Balkan History, Madeleine's War, and NATO's Kosovo," *Serbian Studies: Journal of the North American Society for Serbian Studies* 15, no. 1 (2001): 77–102, <http://www.serbianstudies.org/publications/pdf/V0115>–

1_Bardos.pdf.

7. Organization for Security and Co-operation in Europe (OSCE), Office for Democratic Institutions and Human Rights (ODHIR), *Kosovo/Kosova as Seen, as Told: An Analysis of the Human Rights Findings of the OSCE Kosovo Verification Mission, October 1998 to June 1999* (Warsaw, Poland: OSCE, 1999), cover memo, http://webcache.googleusercontent.com/search?q=cache:74_xAObauVMJ:www.osce.org/odhr/17774e.
8. North Atlantic Treaty Organization (NATO), "NATO's Role in Relation to the Conflict in Kosovo," updated July 15, 1999, <http://www.nato.int/kosovo/history.htm>.
9. Miranda Vickers, *The Albanians: A Modern History* (London: I. B. Tauris, 2006). Originally published 1995.
10. Warren Hoge, "Russia Objects to UN Plan for Kosovo as 'One-Sided,'" *New York Times*, March 20, 2007, <http://www.nytimes.com/2007/03/20/world/europe/20nations.html>; Judy Dempsey, "Diplomats to Increase Pressure on Serbia to Accept Kosovo Plan," *New York Times*, April 18, 2007, <http://www.nytimes.com/2007/04/18/world/europe/18kosovo.html>.
11. "Thaci Refuses to Confirm Independence Date," *France 24*, February 16, 2008, <http://www.france24.com/en/20080215-thaci-refuses-confirm-independence-date-serbia-kosovo/>.
12. Ibid.
13. Reuters, "Tadic Vows to Preserve Kosovo," *France 24*, February 15, 2008, <http://www.france24.com/en/20080215-tadic-vows-preserve-kosovo-kosovo-serbia/>.
14. "Thaci Refuses to Confirm Independence Date."
15. Dan Bilefsky, "Kosovo Declares Its Independence from Serbia," *New York Times*, February 18, 2008, <http://www.nytimes.com/2008/02/18/world/europe/18kosovo.html>.
16. "Serbia Planning Wholesale Rejection of Kosovo State," *Sydney Morning Herald* (Australia), February 13, 2008, <http://www.smh.com.au/news/world/serbia-planning-wholesale-rejection-of-kosovo-state/2008/02/13/1202760333880.html>.
17. Ibid.
18. Slobodan Lekic, "Serbia PM: West Seeks 'Slave-Like' Status for Serbia," Associated Press, February 15, 2008; Jovana Gec, "Serbia to Fight Kosovo Independence," Associated Press, February 16, 2008, http://www.boston.com/news/world/europe/articles/2008/02/16/serbia_to_fight_kosovo_independence/.
19. "Thaci Refuses to Confirm Independence Date."
20. Bilefsky, "Kosovo Declares Its Independence from Serbia."
21. Anastasijevic, "Joy in Kosovo, Anger in Serbia."
22. Tzortzi, "Serbia Pledges Long-Haul Fight over Kosovo"; Anastasijevic, "Joy in Kosovo, Anger in Serbia."
23. Tzortzi, "Serbia Pledges Long-Haul Fight over Kosovo."
24. Bilefsky, "Kosovo Declares Its Independence from Serbia."
25. "Belgrade-Serbia," video of the attack on the US Embassy 0:01:59, No Comment TV, February 17, 2008, <http://www.youtube.com/watch?v=V6WnspPzWmo>; Tzortzi, "Serbia Pledges Long-Haul Fight over Kosovo"; "Rioters Attack US Embassy in Belgrade after Kosovo Protest Rally," Radio Free Europe/Radio Liberty.
26. Simon Roughneen, "Serbia, Ally Reject Sovereign Kosovo," *Washington Times*, February 18, 2008, <http://www.washingtontimes.com/news/2008/feb/18/serbia-ally-reject-sovereign-kosovo/>.
27. Anastasijevic, "Joy in Kosovo, Anger in Serbia."
28. Julian Borger and Peter Beaumont, "Angry but Pragmatic, Protesters Fly the Flag for Nationalism," *Guardian* (London), February 19, 2008, <http://www.guardian.co.uk/world/2008/feb/19/kosovo.serbia1>; "US, European Powers Recognize Kosovo: Rift with Russia, China Apparent in Security Council Debate," MSNBC, February 18, 2008, http://www.msnbc.com/id/23219277/ns/world_news-europe/t/us-european-powers-recognize-kosovo/.
29. "Western States Hail Newcomer," *Oxford Analytica*, February 19, 2009.
30. "US, European Powers Recognize Kosovo," *MSNBC News*.
31. Elie Tzortzi, "Serbs Vent Ire on Kosovo, Western Backers," Reuters, February 18, 2008, <http://www.reuters.com/article/2008/02/18/idUSL18637552/>; Nick Thorpe, "Tension on New Kosovan Border," BBC, February 21, 2008, <http://www.bbc.co.uk/2/hi/europe/7256549.stm>.
32. "Fresh Clashes Reported in Serbian Capital, Slovene Shopping Mall Evacuated," Radio B92, in translation at *BBC Worldwide Monitoring*, February 18, 2008, <http://www.bbc.co.uk/> (site discontinued).
33. F. Berruyer, "NATO Troops Seal Kosovo Border," *France 24*, February 20, 2008, <http://www.france24.com/en/20080220-nato-troops-seal-kosovo-border-kosovo-independence/>.
34. "Special State Department Teleconference Briefing on Kosovo," Briefer: Under Secretary of State for Political Affairs R. Nicholas Burns, Federal News Service, February 18, 2008.

Image Credits

Chapter 1: Who Poisoned Karinna Moskalkenko?

Page 9 (left and right): AP Photo/Efrem Lukatsky

Page 11: Matt Cardy/Getty Images

Chapter 2: The Anthrax Killer

Page 22 (top and bottom): Courtesy of the Department of Justice

Page 24 (left and right): Courtesy of the Department of Justice

Page 25 (left and right): Courtesy of the Department of Justice

Page 26: Courtesy of the Department of Justice

Page 27: Courtesy of the Department of Justice

Page 28: Courtesy of the Department of Justice

Chapter 3: Cyber H₂O

Page 44: Map Data © 2013 Google

Page 44 (inset): Image © Bluesky

Chapter 4: Is Wen Ho Lee a Spy?

Page 65: AP Photo/LM Otero

Chapter 5: Jousting with Cuba over Radio Marti

Page 85 (top): © Bettmann/CORBIS

Page 85 (bottom): AP Photo/Cubadebate, Roberto Chile, File

Page 90: Map Data © 2013 Google

Chapter 6: The Road to Tarin Kowt

Page 106: Capt. Claudia Peña Crossland

Page 108 (left and right): Capt. Claudia Peña Crossland

Chapter 7: Who Murdered Jonathan Luna?

Page 125: Reproduced with the permission of the FBI

Page 126: Reproduced with the permission of the FBI

Chapter 8: The Assassination of Benazir Bhutto

Page 144: AP Photo/Shakil Adil

Page 145: AP Photo/Lefteris Pitarakis

Page 150 (top and bottom): REUTERS/Reuters TV

Chapter 10: The Atlanta Olympics Bombing

Page 184: Reproduced with the permission of the FBI

Page 189: AP Photo/Greg Gibson

Chapter 12: Colombia's FARC Attacks the US Homeland

Page 219: AP Photo/Scott Dalton

Page 220: AP Photo/APTN/Noticias Uno

Chapter 13: Understanding Revolutionary Organization 17 November

Page 242: AP Photo

Page 243: Keystone/Stinger/Getty Images

Page 244: AP Photo/HO/Elfttherotypia

Page 247: Wiki Phantis

Chapter 14: Defending Mumbai from Terrorist Attack

Page 263: AP Photo/Rajesh Nirgude

Chapter 15: Iranian Meddling in Bahrain

Page 294: United States Navy photo by Chief Mass Communication Specialist Julian Carroll

Page 295 (left): <http://bahrain.viewbook.com/> [CC-BY-SA-3.0 (www.creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons

Page 295 (right): By Bahrain in Pictures (<http://bahrain.viewbook.com/>) [CC-BY-SA-3.0 (www.creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons

Chapter 16: Shades of Orange in Ukraine

Page 313 (left and right): Wikimedia Commons

Page 316: www.kremlin.ru

Page 318: Wikimedia Commons

Page 322 (all): Wikimedia Commons

Chapter 17: Violence Erupts in Belgrade

Page 332: AP Photo/Marko Drobnjakovic

Page 338: REUTERS/Nikola Solic